Digital Onboarding: Where Convenience, KYC and Customer Risk Collide

Elizabeth Anne Caddle
Portfolio sample | September 2026

Digital onboarding can make financial services quicker and easier. It can also give firms more confidence than the evidence warrants: the checks may be complete while questions about risk, independence and understanding remain.

From the customer's side, the process appears simple. Upload identification, wait while the checks run, then move on. When it works, it is quicker than passing documents between staff or waiting days for a routine check to clear.

The convenience is real. So is the neat audit trail. Yet a completed journey can make a messy situation look far cleaner than it is.

A customer may reach the end without fully understanding the product. Someone else may be steering the answers or completing part of the form. A document may clear the system without being genuine, accurate or consistent with the customer's circumstances. The application is marked complete, but the record may say nothing about confusion, vulnerability or pressure.

Once that happens, this is no longer just a design problem. KYC, financial crime, vulnerability and customer understanding may all be in play.

What the system cannot see

In a branch or over the phone, staff may notice things that never appear in a data field: a long pause before an answer, a voice in the background, a customer who sounds frightened, or an explanation that changes each time it is repeated.

In one of my banking roles, I refused to process a payment because I could hear somebody coaching the customer in the background. Nothing on the screen made the transaction look unusual. The conversation told me that the customer was not acting independently.

Documents can create the same unease. I have seen payslips with blurred, misaligned text and basic wording errors. One showed 'Company No:' as 'Company Numb:'. The person behind the document also changed his account each time we spoke. The mistake alone proved nothing, but it was one more reason to stop and look properly.

Human contact is no guarantee that a problem will be caught. Staff overlook things too. It does, however, create an opportunity to notice that something does not fit and ask another question before the transaction goes through.

An automated route sees only the signals it was designed to capture: a form submitted, a document uploaded, a verification passed or failed. Those records matter, but they are not the whole story. Firms need to know what the system cannot detect and what, if anything, is in place to compensate for it.

KYC is more than an identity check

Customers can be forgiven for treating KYC as one more obstacle between them and the service they came for. For the firm, customer due diligence has a wider purpose. Under Regulation 28, the requirements include identifying and verifying the customer, assessing the purpose and intended nature of the relationship or transaction, and conducting ongoing monitoring.[1]

Those duties lead to practical questions. Does the activity make sense for this customer? Are they acting for themselves? Is there anything in the transaction, behaviour or documents that warrants a closer look?

Digital identity verification can answer the identity question well. It can reduce unnecessary handling and delay, and provide reliable evidence that the person is who they claim to be. It cannot establish that the customer understands the product, is acting freely or that the transaction fits their circumstances.

A verified identity is useful evidence, but it is only one part of assessing the customer and the risk presented by the relationship or transaction.

Digital identity helps, but responsibility stays with the firm

The UK's 1.0 digital verification services trust framework was finalised in June 2026. It sets rules for providers seeking certification. Separate government guidance explains how certified and registered services may be used for identity checks under the Money Laundering Regulations.[2][3]

This gives firms a clearer basis for deciding which services they are prepared to rely on. It should also spare some customers from repeatedly producing paper documents or going through the same manual checks.

But this is verification, not a transfer of responsibility. Government guidance says that digital identity can support verification without removing the rest of a firm's obligations under the Money Laundering Regulations.[4]

The provider supplies the service and the verification result. The firm still has to decide what that result means for this customer, this product and this transaction.

---

[1] Regulation 28, Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.
[2] GOV.UK / Office for Digital Identities and Attributes, 'UK digital verification services trust framework', version 1.0, published 3 March 2026 and updated 9 June 2026.
[3] HM Treasury and Department for Science, Innovation and Technology, 'Using digital identities with the Money Laundering Regulations', 26 February 2026.
[4] HM Treasury and Department for Science, Innovation and Technology, 'Using digital identities with the Money Laundering Regulations', 26 February 2026.

A completed journey may still be a poor customer journey

Digital teams are usually asked to remove unnecessary steps and shorten completion times. That is sensible.

Poorly designed forms create errors and exclude people who could have completed the process with clearer wording or a little more flexibility.

The trouble starts when completion is treated as proof of understanding. Someone with low literacy may click through rather than admit they need help. A neurodivergent customer may be overwhelmed by dense wording or an unclear sequence. A person experiencing coercive control may be completing the form under somebody else's watch. An older customer may pass the identity check without fully understanding what they have agreed to.

The system may call the journey a success even if the customer got through it by guessing or while under pressure. Completion data alone cannot show the difference.

The FCA's guidance on vulnerable customers, and its later review of firms' treatment of them, make this difficult to dismiss. Digital journeys need to accommodate customers who require more time, clearer information, help from a member of staff or a route out of the automated process altogether.[5]

That cannot be solved by letting UX, compliance and vulnerability teams examine separate pieces of the journey. If each team signs off only its own work, the gaps between them remain untested.

Some friction has a purpose

Friction is often treated as a design failure. In financial services, however, some interruptions protect the customer, the firm or the wider financial system.

A request for more evidence may be inconvenient but justified. A warning may prevent harm. Manual review may delay an application but catch something the automated checks missed.

The question is whether the friction is proportionate and explained. Repeating a request without saying why feels obstructive. Explaining what the evidence will establish makes the interruption easier to understand, even if it is unwelcome.

Customer understanding is an outcome under the Consumer Duty. The FCA expects communications to be timely and understandable and, where appropriate, tested and monitored. A digital journey falls short if the customer is left guessing why information is required or what happens next.[6]

---

[5] FCA, 'FG21/1: Guidance for firms on the fair treatment of vulnerable customers', 23 February 2021; and FCA, 'Delivering good outcomes for customers in vulnerable circumstances', 7 March 2025.

[6] FCA, 'Consumer understanding: good practice and areas for improvement', 13 March 2026; and PRIN 2A.5, FCA Handbook.

If a firm needs more information, it should explain why. If a case moves to manual review, a vague holding message is not enough. A warning intended to make someone stop and think must be written to have that effect, not merely displayed so the firm can show that it appeared on screen.

The wording is doing part of the work

Wording is often treated as the final layer of a digital project, to be tidied up after the process and controls have been built. By then, important decisions may already have been made.

The words influence what information the customer provides, whether they understand the request and whether they know when to ask for help.

'Complete verification to proceed' tells the customer what the system wants. 'We need to check your identity before we can continue' tells them what is happening.

'Upload source of funds documentation' assumes the customer knows what the phrase means. A clearer version would be: 'We need evidence showing where this money came from. This helps us meet anti-money laundering requirements and check that the transaction matches what you have told us.'

The rewritten versions are not softer and they do not weaken the control. They give the customer a reason instead of an instruction dressed up as compliance language.

That makes it more likely that the right information will be provided first time, while reducing avoidable confusion about what the firm is asking for.

A smooth journey can still hide a weak process

A good digital onboarding journey cannot be judged only by how quickly customers finish it. Firms also need to know where judgement was applied, how unusual or higher-risk cases were handled and what happened when the standard route did not fit.

The useful questions are not flattering ones. Did the information add up when it was considered together? Could a confused or vulnerable customer reach a person? Were warning signs investigated or quietly explained away? Did the technology make the process safer, or merely faster?

The FCA's 2026 review was not specifically about digital onboarding. Even so, it found firms with procedures lacking practical detail, missing records of the purpose and intended nature of business relationships, and no evidence of enhanced due diligence measures. A digital record can capture every step without improving the decision behind it.[7]

[7] FCA, 'Firms' customer due diligence processes and controls: our findings', 8 April 2026.

Convenience and control need not conflict. A process can be quicker and clearer while leaving room to question what does not fit. The risk begins when a polished journey is mistaken for proof that the process behind it is sound.

If all a firm can show is that the customer reached the final screen, it has proved completion, not understanding, independence or a sound control.