Who controls the technology behind UK retail & SME banking?

How much the sector depends on a handful of technology suppliers it cannot fully control — and where that matters most.

Martin De Saulles | Principal Analyst · June 2026

The big picture

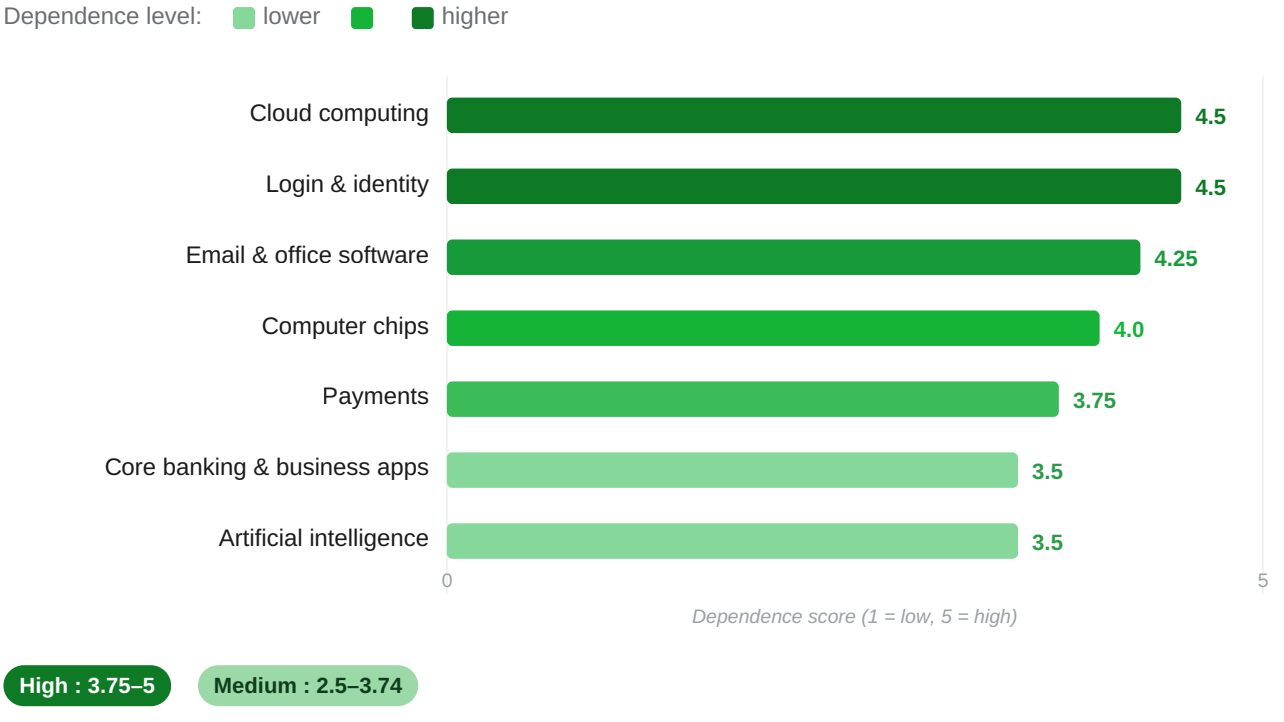
4.0 / 5

HIGH DEPENDENCE

UK retail and small-business banking runs on a small number of mostly US-owned technology suppliers. For the most important parts of the stack, there is no easy way to switch and no home-grown alternative ready to step in. The good news: the everyday payment system and some core banking software are more home-grown than people assume.

We looked at seven layers of technology the sector relies on, and scored each one from 1 (low dependence) to 5 (high). The score weighs how few the suppliers are, whose laws they answer to, how hard they are to switch, and how essential they are to keep the bank running. UK regulators already treat heavy reliance on a few cloud and AI providers as a risk to the stability of the financial system.[7]

Where the dependence sits — the seven layers



Five of the seven layers fall in the “high” band. Cloud and login systems are the most exposed; core banking software and AI are the least.

What this means, in plain terms

The cloud is the biggest single dependence. Almost everything else runs on top of it, it is dominated by three US providers (Amazon, Microsoft, Google), and fewer than 1 in 100 customers switch provider in a given year.[1] If the cloud goes, much of the rest goes with it.

Login and identity is the fastest "switch-off" risk. The systems that let staff and customers sign in are all US-owned, with no UK or European alternative at scale. A single fault can lock people out everywhere at once, with no warning.[6]

UK payments are more home-grown than people assume. The card networks (Visa and Mastercard) are American and handle over 95% of card spending[2] — but the everyday bank-to-bank systems that move most money are run in the UK, and bank-to-bank payments are growing fast (351 million in 2025, up 57%).[3]

Core banking software has real UK and European choices. This is the one layer with a genuine non-US option (for example Thought Machine, 10x, Engine by Starling)[4] — so the sector is not locked in here.

The gap is starting to narrow. Amazon and Microsoft now offer "sovereign cloud" services run inside Europe (Amazon's went live in January 2026).[5] These help, but the parent companies are still American — so they reduce the risk rather than remove it. (One structural fact behind the chip layer: almost all of the world's most advanced computer chips are made in Taiwan.[8])

If a supplier pulled the plug, how fast would it hurt?

SPEED OF IMPACT	LAYER	WHAT HAPPENS
Immediate	Login & identity	Staff and customers locked out across all systems at once.
Within days	Cloud · Email & office	Services that run on the cloud degrade; documents and email stop working.
Weeks	Artificial intelligence	Easiest to replace — alternatives and open models can fill in.
Weeks–months	Core banking	Contracts and UK-based systems give breathing room to move.
Months+	Payments · Chips	Cards would bite, but UK bank-to-bank rails keep working. Chips are a national issue, not a single bank's.

What banks can do about this

LAYER	PRACTICAL STEPS
Cloud	Banks should hold their own encryption keys, so the provider cannot read their data without them. They should keep a tested copy of their most critical systems with a second provider or in a UK/EU "sovereign" region (for example the AWS European Sovereign Cloud, live since January 2026[5]), and write exit rights, data-portability and capped data-removal ("egress") fees into every contract — those fees were cut across the industry in 2024.[1]
Login & identity	This is the top contingency risk. Banks should keep a written, rehearsed fallback for signing in — emergency "break-glass" admin accounts, a back-up identity provider, and offline access for critical staff. They should ask their provider where sign-in data is stored, and secure data-residency commitments in writing.[6]
Email & office	Banks should standardise on open file formats so documents are not locked to one supplier, and keep their own backups. For board, legal and customer-sensitive material, they should consider a UK- or EU-hosted email service rather than the default US cloud.[6]
Core banking	This is where banks have real choice. They should favour UK or European core-banking platforms (for example Thought Machine, 10x, Engine by Starling[4]) for new builds, and write data-portability and exit-assistance clauses into contracts so they can move if they need to.
Payments	Banks should route everyday payments over the UK-run bank-to-bank rails (Faster Payments) where they can, and offer "pay by bank" at checkout to lean less on cards.[3] They should map exactly where they rely on Visa and Mastercard so the board can see the exposure plainly.[2]
AI	Banks should keep AI suppliers swappable: a provider-neutral layer between their apps and any one model, with an open-weight model on standby as a fallback. It is the cheapest resilience on this list — and regulators expect them to manage the dependency.[7]

Sources

1. Competition and Markets Authority — *Cloud services market investigation: final decision* (July 2025) and update on remedies (March 2026). https://assets.publishing.service.gov.uk/media/688b20e6ff8c05468cb7b120/summary_of_final_decision.pdf
2. Payment Systems Regulator — *Market review of card scheme and processing fees: final report* (MR22/1.10, March 2025). https://www.psr.org.uk/media/sogjjvl4/mr22-110-card-sp-fees-mr-final-report-publication-redacted-mar-2025-updated.pdf
3. Open Banking Ltd — *Open Banking in 2025: Now Part of the UK's Everyday Financial Life* (January 2026). https://www.openbanking.org.uk/insights/open-banking-in-2025-now-part-of-the-uks-everyday-financial-life/
4. Companies House records and company filings — UK and European core-banking providers (Thought Machine, 10x Banking, Engine by Starling). https://find-and-update.company-information.service.gov.uk/

5. Amazon Web Services — *Opening the AWS European Sovereign Cloud* (15 January 2026). https://aws.amazon.com/blogs/aws/opening-the-aws-european-sovereign-cloud/
6. Microsoft — *EU Data Boundary: continuing data transfers that apply to all services* (2026); Microsoft Entra (Azure AD) incident report (2021). https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-transfers-for-all-services
7. Bank of England & FCA — *Artificial intelligence in UK financial services* survey (2024): https://www.bankofengland.co.uk/report/2024/artificial-intelligence-in-uk-financial-services-2024. Critical Third Parties regime (PS24/16, in force January 2025): https://www.fca.org.uk/publications/policy-statements/ps24-16-operational-resilience-critical-third-parties-uk-financial-sector
8. Congressional Research Service — *Semiconductors and the CHIPS Act: the global context* (R47558); company filings (SEC). https://www.congress.gov/crs-product/R47558

How we did this. We scored seven technology layers on four things — how concentrated the suppliers are, whose laws they answer to, how hard they are to switch, and how essential they are. Every figure comes from the primary sources listed above. Scores are bands, not exact measurements. Full evidence record available on request.

Information Matters · informationmatters.net