Fintech Den™ White paper

BaaS Independence: Multi-Bank Routing and Safe Migration

Keep your product running when a sponsor bank changes the terms, with a second bank ready and a tested way to move.

Summary

Many fintechs reach customers through a single sponsor bank, often by way of a banking-as-a-service platform in the middle. That works well until the bank raises its fees, narrows the programmes it will support, or is told by its regulator to slow down. At that point the fintech finds out how much of its business it doesn't control.

Fintech Den™ helps fintechs reduce that dependence. We design and build a banking layer that your product talks to instead of talking to one bank directly, so a second or third bank can be added, volume can be split, and a move can be planned rather than rushed. When a move is needed, we run it as a short, structured migration with data portability and minimal disruption for your customers.

We're a new company, and we'd rather be straight with you about that. This paper sets out the problem as we see it, how we'd approach it, the rules in the US, UK and EU that shape it, how we handle your data, and a first project small enough to judge us on.

Data protection is usually the first thing UK and EU buyers check, so we'll say it up front: we comply with the UK GDPR and the EU GDPR, and we're registered with the UK Information Commissioner's Office. The GDPR section below explains what that means for your project, from where your data is hosted to how we'd tell you about a breach.

The problem

In 2024 a banking-as-a-service middleware provider in the US collapsed, and end customers of several fintech apps were cut off from their money for months while banks and administrators tried to work out who was owed what. The underlying issue was not the app. It was that the records of who owned each balance sat in one intermediary's systems, and nobody else could reconcile them quickly.

Since then, sponsor banks have come under much closer supervision, and many have tightened their programmes, raised their prices or exited fintech partnerships altogether. A fintech with one bank behind it can be given a few months' notice to find another, with all the account, card and payment integrations that implies.

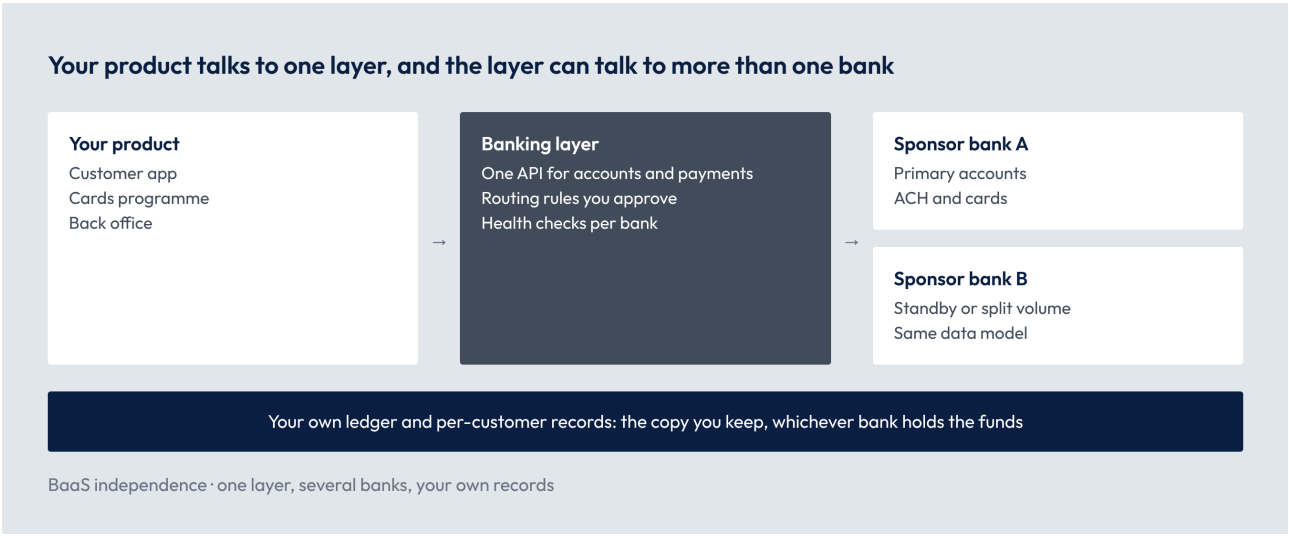
Moving is hard because most integrations were never built to move. Account numbers, card programmes, payment rails, KYC records and ledgers are tied to one partner's APIs and data model. Without a plan, a migration means rewriting large parts of the product under time pressure, while customers wait.

How we would approach it

We'd start by mapping exactly what depends on your current bank or BaaS platform: accounts, cards, payment rails, KYC data, the ledger and the reconciliation files. Then we'd put a banking layer between your product and the bank, with your own ledger and records underneath it, so the bank becomes a connection you can change rather than the foundation of your product.

In most cases the build has three parts:

Part	What it does	What we'd aim for
Multi-bank layer	One internal API for accounts, payments and cards, with connectors to two or three sponsor banks	A second bank you can switch to or split volume with, without rebuilding your product
Your own records	A double-entry ledger and per-customer records that you hold, reconciled daily with each bank	You can always show who owns what, whichever bank holds the funds
Migration sprints	Structured moves from one BaaS provider or bank to another, usually in about 60 days once both sides are ready	Customers moved in waves, with balances checked at every step



BaaS independence · one layer, several banks, your own records

The diagram shows the idea. Your product only knows the banking layer. The layer routes each account or payment to a bank according to rules you approve, and if one bank pauses a service or degrades, traffic can move to another. Your ledger sits underneath, so balances never depend on a single partner's records.

Routing across banks is not free: each bank has its own onboarding, limits and compliance expectations, and some products, such as card programmes, take longer to set up twice. We'd help you decide which services really need a second bank and which only need a tested exit plan.

The rules behind BaaS in the US, UK and EU

Regulators in all three markets now expect firms to know where customer money is, to keep their own records, and to be able to survive the failure of a key partner. This is a summary for discussion, not legal advice.

Market	Rule	Where it stands (November 2026)	What it means for the build
US	FDIC proposal on recordkeeping for custodial deposit accounts in bank-fintech arrangements	Proposed in October 2024; on the FDIC's long-term agenda, with no date for a final rule	Daily per-customer records that a bank can reconcile, whichever bank holds the funds
US	Bank Secrecy Act and AML programmes, plus sponsor-bank oversight of fintech partners	In force, with closer scrutiny since 2024	KYC and monitoring records that can move with your customers if you change bank
UK	FCA safeguarding rules for payment and e-money firms: daily checks, monthly returns, annual audits	In force since 7 May 2026	Safeguarding figures that stay correct throughout a migration
UK	FCA operational resilience rules: important business services and impact tolerances	Firms had to be able to stay within their impact tolerances by 31 March 2025	A tested way to keep important services running if a bank or provider fails
EU	Digital Operational Resilience Act (DORA)	Applies since 17 January 2025	Exit plans for critical ICT providers and a register of third-party arrangements

UK and EU GDPR compliance

Moving customers between banks means moving their personal data, so it has to be clear who holds what and on what basis. We comply with the UK GDPR, alongside the Data Protection Act 2018, and with the EU GDPR. On client projects where we handle personal data, you're the controller and we act as your processor. Here's what that means in practice.

Area	What we do
Data processing agreement	We sign one with every client, covering everything Article 28 of the UK and EU GDPR requires. We act only on your documented instructions, and everyone on your project is bound by confidentiality. Our standard agreement is ready for your legal team to review.
Collecting less	Systems collect only the personal data they need. By default we build and test with synthetic or masked data, not live customer records.
Where data lives	Production systems run in your own cloud account, in the UK or EU region you choose.
Migrations	Customer data is moved between banks or providers only under your instructions and the agreements you hold with them, in encrypted transfers, with a record of what moved and when.

Area	What we do
Access and transfers	Any access to real personal data is agreed with you first, limited to named people, logged, and removed when the task is done. If access ever involves a transfer outside the UK or EU, it's covered by the EU standard contractual clauses or the UK international data transfer agreement. Both are ready to sign.
Security	Encryption in transit and at rest, least-privilege access, logging, and code review on every change.
Sub-processors	We tell you which sub-processors we use, and add new ones only with your prior authorisation.
People's rights	We help you respond when people ask to see, correct or delete their data.
Breaches	If we become aware of a personal data breach affecting your data, we tell you without undue delay, so you can meet the 72-hour deadline for reporting it to the ICO or your EU supervisory authority.
Assessments and audits	We support your data protection impact assessments, give you the information you need to show compliance, and allow audits.
End of the work	We return or delete your personal data, whichever you choose.

Where we stand on registrations and certifications. We'd rather be precise than impressive.

Item	Where it stands
ICO (UK)	Registered with the Information Commissioner's Office.
EU to UK data flows	The EU recognises UK data protection law as adequate. The European Commission renewed that decision in December 2025, and it runs until December 2031.

For EU firms under DORA. If you're an EU financial entity, our DORA information sheet gives you what you need to record us in your register of ICT third-party providers: our company details, the services we provide, where data is processed and the subcontractors we use. We'll also work through the DORA contract terms with your team.

How we work

Since we can't yet show you years of past projects, we'd like to show you our process instead, in writing, before you commit.

The people you'll work with. You deal directly with our leadership. There's no account manager in between.

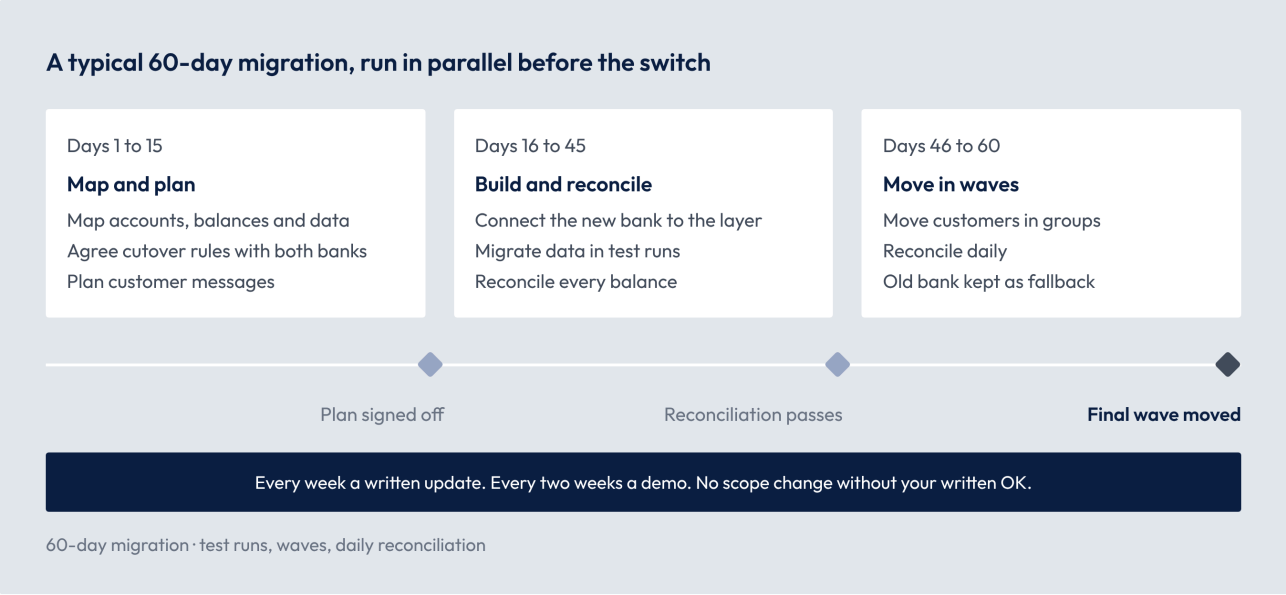
Role	What they look after on your project
Chief Executive Officer	The relationship, scope, security and data protection, and fit with your bank partnerships
Chief Technology Officer	Banking-layer and ledger design, migration planning, technical risk, final technical sign-off, and sometimes the relationship and scope
Head of Engineering	Bank and provider integrations, data migration, reconciliation testing and releases
Head of Visual Design	Customer messaging during a move, back-office screens and migration dashboards

Company and working hours. Fintech Den™ is a trading name of ROMBI PIXEL LTD, a UK company registered in England and Wales (no. 15947340) with its registered office in Bury St. Edmunds. We run on Central European Time (CET), so our working day overlaps with business hours across the UK and EU. For US clients, our afternoon overlaps with the East Coast morning, and we schedule calls in that window.

The practical side. We quote and invoice in euros, US dollars or pounds, whichever suits your finance team, and EU clients can pay by SEPA transfer to our euro account. Proposals spell out scope, milestones, payment points and VAT treatment, and payments are tied to milestones you can check. Our master services agreement is ready for your legal team, and we're open to discussing governing law and other terms.

Habits you can hold us to. We send a written summary within one working day of every call. You get a short written update every week and a demo every two weeks. Risks go in a shared log as soon as we spot them, and nothing changes scope without your written agreement.

What a migration usually looks like. Once both banks are ready to work with us, a typical move takes about 60 days. The timing depends heavily on the banks, and we'll be honest with you about it from the start.



If you aren't moving yet, the same work can be done calmly as a contingency: the layer and a second bank connection are built and tested, and the switch is only made if you need it. You can stop at any checkpoint and keep everything we've produced so far.

Starting a conversation

The first call is mostly us listening. We'll probably ask about:

1. Which bank or BaaS platform you depend on today, and for which services.
2. Whether you hold your own ledger and per-customer records, or rely on your partner's.
3. Whether you've had notice of changes to fees, limits or your programme.
4. Which services would hurt most if they stopped for a day.
5. Where your data has to be hosted.

If it looks like we can help, we'll suggest one of these as a first step. Timings are typical, not fixed, and we'll confirm them in a written proposal.

Option	Typical length	What you'd receive
Dependency review	About 2 weeks	A map of everything tied to your current bank, the risks, and a contingency or migration plan with a fixed scope
Banking layer and second bank	About 3 months	Your own ledger and the banking layer in place, with a second bank connected and tested
Migration sprint	About 60 days once both banks are ready	Customers, balances and records moved to the new bank in waves, with daily reconciliation

If it doesn't look like a good fit, we'll tell you, and where we can, we'll point you to someone better placed.

Before the call, we're happy to send our trust pack: our data processing agreement and the EU and UK transfer clauses, plus the DORA information sheet if you're an EU financial firm. We are working towards IASME Cyber Assurance and the NCSC-backed Cyber Essentials certification.

To arrange a call, email contact@fintechden.com. We'll reply within one working day.

Sources

- FDIC: proposed requirements for custodial deposit accounts
- Unified Agenda: status of the FDIC custodial account rule
- FCA: changes to payment safeguarding rules
- FCA: operational resilience
- ESAs: DORA registers of information and critical ICT providers
- Hunton: European Commission renews UK adequacy decisions
- ICO: contracts between controllers and processors
- GDPR Article 33: notifying a personal data breach

Ready to Talk About Your Project?

Book a discovery call and we'll mostly listen. Not sure which service fits? Start with a fixed-price Discovery Sprint. We work on Central European Time and reply within one working day.

Book a discovery call | fintechden.com

Fintech Den™

Fintech Den™ is a trading name of ROMBI PIXEL LTD.
Registered in England and Wales. Company No. 15947340.
Registered office: Suite A, 82 James Carter Road, Bury St. Edmunds, IP28 7DE, United Kingdom.
Contact: contact@rombipixel.com

© 2026 Fintech Den™. All rights reserved.

Find us on social media LinkedIn Twitter