obconnect
WE DELIVER OPEN BANKING

From Open Banking to the Corporate Data Sharing Ecosystem: Why Trust Infrastructure Matters

Produced in cooperation with RAIDIAM

Summary of content:

1. The shift from open banking as a compliance initiative to a broader data-sharing ecosystem
2. Why secure data exchange is becoming increasingly important for corporates and financial institutions
3. The role of banks, obconnect and ecosystem participants in enabling trusted data and payment flows
4. How Confirmation of Payee, account information and open banking payments fit into the bigger picture
5. The infrastructure challenge: how to make data sharing secure, scalable and easy to adopt
6. How Raidiam Connect supports trusted, standards-based access between organisations, applications and APIs

1 The shift from open banking as a compliance initiative to a broader data-sharing ecosystem

With the level of financial inter-connectivity we see in today's world, and the expectations that Customers now have around data sharing or payment processing, it's easy to forget that Open Banking is still a relatively new phenomenon.

In the UK, as of December 2025, there were 16.5million user connections established (that's a whopping 36% year on year increase), and an eye-watering 24 billion API calls processed across the ecosystem, all of which has now driven system reliability across the market upwards of 99.5%. At that kind of scale, it has quietly become critical national infrastructure.

For businesses, secure data exchange is no longer simply a regulatory or technical consideration. It is a business-critical capability: supporting more efficient payment journeys, stronger fraud controls, better customer experiences and the ability to launch new services with confidence.

The challenge is that data sharing becomes more complex as the ecosystem expands. Organisations need more than an API connection: they need clarity over who is participating, what data or payment permissions apply, how access is authenticated and governed, and how services can operate reliably at scale. Trust infrastructure – the standards, identity, security and governance that sit beneath data exchange – is what makes this possible.

In practice, this can mean helping finance and treasury teams gain a clearer view of accounts and cash positions, make payments more efficiently, verify beneficiaries before funds are sent, and connect securely with banks and service providers. The services may differ, but they rely on the same foundation: trustworthy identity, explicit permissions, interoperable standards and reliable operational controls.

In 2016, the UK's CMA open-banking remedy required the UK's largest current-account providers to make customer-permissioned data available to authorised third parties. Its objective was to improve competition and consumer choice.

The UK's open banking ecosystem provides a useful proof point. Regulation created the initial momentum, but common technical standards, participant requirements and operational infrastructure enabled different organisations to connect and transact with confidence at scale.

The enduring lesson is not that regulation alone creates an ecosystem. It is that

regulation, standards, governance and effective implementation must work together. Standards such as FAPI, together with secure participant registration, directory services and customer-experience requirements, helped turn the ambition for interoperable data sharing into a practical market capability.

A decade on, the broader lesson applies beyond retail banking: durable data-sharing ecosystems depend on trusted implementation. For businesses, financial institutions and their technology partners, the opportunity is to apply those lessons to broader data, payment and verification journeys – making them secure, scalable, interoperable and straightforward for every participant to adopt.

2 Why secure data exchange is becoming increasingly important for corporates and financial institutions

Here's the flip side of all that growth though, every one of those 24 billion API calls is also a transaction where a security gap in any single participant, whether they're a bank, a TPP, or an intermediary, can cascade straight through the value chain. Interconnectivity is a double-edged sword. It is what makes the ecosystem valuable, and it's exactly why secure by design has to be non-negotiable rather than a box to tick after the event.

Regulatory developments, including the EU's Digital Operational Resilience Act (DORA), reflect the growing focus on operational resilience and technology-supply-chain risk. For organisations operating across markets, this reinforces a practical reality: secure data sharing must be designed into the ecosystem from the start, rather than added after services have already scaled.

As data and payment ecosystems become more interconnected, the consequences of a weakness at any point in the chain can extend beyond a single organisation. Banks, payment providers, fintechs, technology partners and other intermediaries therefore need to consider security, resilience and third-party risk as shared responsibilities.

3 The role of banks, obconnect and ecosystem participants in enabling trusted data and payment flows

Banks remain the custodians at the centre of all this. They hold the accounts, they carry the settlement risk, and increasingly they're the trust anchor everyone else builds on. The market expectations on banks have grown well past exposing an API because the CMA mandated them to do so. Banks are now expected to hold always-on availability, share liability when APP fraud slips through, and verify every participant's regulatory status before an API call gets honoured. This is a much bigger remit than the original mandate stipulated.

Then there's the layer in between; the TPPs, fintechs, and infrastructure providers like us, who build upon these standards the products people use daily. This is where most of the real innovation happens, and it's also where most of the real risk lies, because every layer built on top of FAPI or ISO 20022, must ensure that the integrity of the standards are upheld. Get that wrong, and you've quietly eroded the trust the whole ecosystem relies on.

What has changed is the growing expectation that accountability for security and resilience is shared across the ecosystem. Trust here is a shared obligation, not a baton passed from bank to fintech to processor. Every one of those 16.5 million connections is a moment where that shared accountability either worked, or it didn't. The standards give everyone a common language, the implementations that enable the millions of transactions is where the work lies.

4 How Confirmation of Payee, account information and open banking payments fit into the bigger picture

Open Banking gets talked about as one thing; however, it's really three capabilities that all matured alongside each other, each solving a different piece of the trust puzzle. Account Information was the first, the read-only window into your own data that kicked off the first wave of accounting, budgeting apps, and affordability tools. Payment Initiation is the more commercially interesting relative, letting a customer pay straight from their bank account instead of routing through card rails. This is now where the growth is really happening, with sweeping VRP volumes nearly doubling in 2025,

and commercial VRP wave 2 finally going live in November with Tink, Visa, and many more in the mix.

Confirmation of Payee sits apart from both, CoP isn't an Open Banking capability at all, it's a PSR-mandated Pay.UK service solving a much older problem: 'am I sending this money to the right beneficiary?' As PIS and VRP have scaled though, CoP has quietly become the anchor underneath all of it. The PSR increased their mandate from six banking groups to nearly 400 more firms, resulting in Faster Payments CoP coverage increasing from 92% to 99%, this is because a payment ecosystem without payee verification at that scale is just fraud waiting to happen.

Together, these capabilities address complementary needs: AIS can provide visibility of account data, PIS can enable account-to-account payment journeys, and CoP can help reduce the risk of misdirected payments. They are distinct services, with different rules, participants and implementation models, but each depends on trusted participation, secure access and reliable infrastructure.

This is still however far from finished business, in the 1st half of 2024 alone APP fraud losses were still upwards of £213 million, despite the market coverage of CoP being close to 100%. As fraudsters get smarter, and AI ramps up, the trust frameworks will need to keep pace and get stronger, not stand still.

5 The infrastructure challenge: How to make data sharing secure, scalable and easy to adopt

Ease of adoption relies on frictionless Customer Experience. The standards are what give you a shared language, FAPI, ISO 20022, CoP, the Directory, none of these standards alone actually solves anything by themselves though. The standards don't build the product that the Customers want & need or stand up the scalable infrastructure that ensures a reliable & resilient service giving confidence to millions of users that their payment will reach its desired destination quickly.

The trade-off between frictionless journeys vs security is a constant UX battlefield, played out continually between Fraud/Security teams and their Colleagues championing the least click-throughs in a customer journey. The criticality of strong frictionless Customer Experience is exactly however what makes or breaks the success of new technology adoption. When you combine

strong security, with scalable platform infrastructure, alongside an obsession on slick Customer Experience, those are the ingredients on which the success of a new data exchange or new payment proposition is dependent upon and is exactly the space where we do the hard work, meaning that our Clients don't have to.

Trust does not mean adding friction. It means creating a consistent, reusable way for participants to establish identity, permissions and accountability, so secure data-sharing services can scale with confidence.

6 How Raidiam Connect supports trusted, standards-based access between organisations, applications and APIs

Open standards make interoperability possible, but an ecosystem also needs a trusted way to establish who is participating, what they are authorised to do, and how access is managed consistently as the network grows.

Raidiam Connect is designed to support this trust layer: enabling standards-based connectivity between organisations, applications and APIs, while helping ecosystem participants manage identity, permissions and secure access at scale. It can support common rules for participation and provide a consistent way for members to discover, verify and connect with one another.

Rather than requiring every participant to build and maintain bespoke trust relationships with every other participant, a shared approach can reduce complexity and support more consistent governance across the ecosystem.

For corporates, banks and service providers, that matters because secure data sharing needs to be practical to adopt as well as robust by design. Trusted access infrastructure can help create the conditions for new payment, data and verification services to scale with greater confidence.

The next phase of data sharing will be defined not simply by the APIs organisations expose, but by the trust, governance and operational resilience that allow participants to use them with confidence.

Open Banking expertise, built for real-world payments.

Built from the core of Open Banking — not a bolt-on — obconnect is an FCA-regulated, all-in-one Open Banking provider founded in 2019. We deliver Confirmation of Payee, Verification of Payee and Open Banking technology to over 55 banks and institutions worldwide.

Part of the PayPoint Group

obconnect.io

Pioneers in data sharing ecosystems.

Founded in London in 2016 by Ralph Bragg and Barry O'Donohoe, Raidiam helped design the UK's Open Banking trust infrastructure: the world's first regulated open data ecosystem. Today we operate trust infrastructure for national-scale schemes around the globe.

raidiam.com