Open Banking: The Data Liberation Dilemma

Your bank knows everything about your money – once the door opens, who benefits?

Digital Finance

Why Does Your Bank Refuse to Share Your Own Data?

The Ownership Question

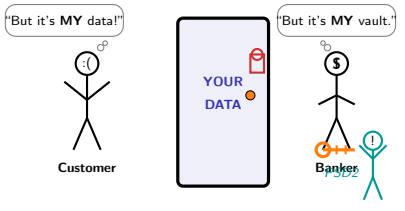
Every time you buy coffee, pay rent, or receive your salary, your bank records it. Over years, this data paints a complete picture of your life. But you cannot take it with you.

Why banks hold your data hostage:

- Transaction history is a competitive moat – it predicts your behavior
- Sharing data with competitors erodes the information advantage
- Legacy systems were never designed for data portability
- Banks profit from being the sole custodian of your financial identity

Why this matters now:

- Regulators decided customers OWN their data, not banks
- Technology makes secure data sharing possible via APIs
- New companies want to use YOUR data to serve YOU better
- The battle is over who controls the relationship – bank or customer



Your bank recorded every coffee you bought.
Now the regulator says you can take that data elsewhere.

Banks accumulated decades of customer data and treated it as a competitive asset – open banking challenges the assumption that custody equals ownership.

Have You Ever Wished All Your Accounts Were in One Place?

Reflection Prompt

Think about every financial account you have – your main bank account, a savings account, maybe a payment app, a trading platform, a credit card.

Can any single app show you all of them at once? If not, how do you track your total financial position – spreadsheet, mental math, or do you simply not know?

Before open banking, the answer was almost always "no." Each bank guarded its data behind its own login, its own app, its own interface. Seeing your complete financial picture required logging into every account separately.

Now imagine a world where:

- One app shows balances from all your banks in a single dashboard
- A lending platform checks your income by reading your bank transactions directly – no payslips needed
- You pay for something online and the money moves directly from your bank account, bypassing card networks entirely
- A budgeting tool categorizes your spending across all accounts automatically

This is what open banking enables. The technology exists. The regulation mandates it. The question is whether **you trust it enough to hand over the keys to your financial life**.

Open banking was born from a simple frustration: your money is in five places, but no single app can see it all – until now.

What Is Open Banking and How Does It Differ from Traditional Banking?

Dimension	Closed Banking	Open Banking	Open Finance
Data access	Bank only	Bank + licensed TPPs	All financial providers
Customer consent	Not needed (internal)	Explicit opt-in (90-day)	Explicit opt-in
API availability	None (proprietary)	Mandated (PSD2)	Mandated (FIDA proposal)
Scope	Payment accounts	Payment accounts	Pensions, insurance, investments
Data portability	None	Transaction history	Full financial profile
Competition model	Bundled (one bank)	Unbundled (specialists)	Fully modular
Innovation driver	Internal R&D	Third-party developers	Cross-sector platforms
Customer control	Low	Medium (consent)	High (full portability)

The progression of openness

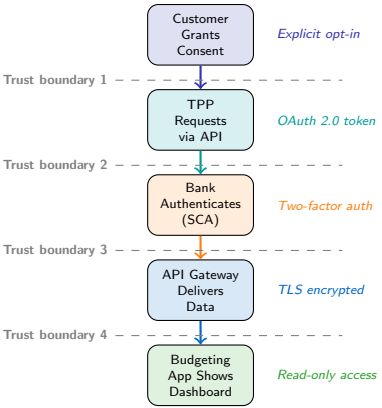
- **Closed banking:** Banks hold all data internally. No third-party access. Innovation happens only inside the bank – slowly.
- **Open banking:** Regulation forces banks to share payment account data via APIs. Third parties can read your transactions and initiate payments – with your consent.
- **Open finance:** The next frontier. Extends API access beyond bank accounts to pensions, insurance, and investments.

The foundational principle

Banks are data **custodians**, not data owners. The customer decides who sees their data, for how long, and for what purpose. This inverts the traditional power relationship.

Open banking is not a product – it is an infrastructure shift that changes who can access financial data and what they can do with it.

Follow Your Data from Bank Vault to Budgeting App



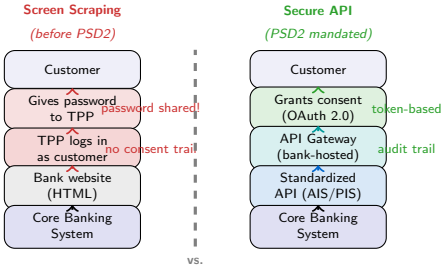
Five steps, four trust boundaries

- **Consent:** The customer explicitly authorizes the third-party provider (TPP) to access specific account data. Consent is granular – not a blanket "yes to everything."
- **API request:** The TPP sends a request using an OAuth 2.0 token. The TPP never sees or stores the customer's bank password.
- **Authentication:** The bank verifies the customer's identity via Strong Customer Authentication (SCA) – two of: something you know, have, or are.
- **Data delivery:** The bank's API gateway sends encrypted transaction data. Only the data the customer consented to share is transmitted.
- **Display:** The budgeting app shows the data in a dashboard. The app has read-only access – it cannot move money or modify the account.

Key insight: The customer authenticates with the **bank**, not with the third party. The bank remains the gatekeeper of identity.

Your data crosses four security boundaries before reaching the budgeting app – each boundary requires a different trust mechanism.

Screen Scraping or Secure APIs – Which Would You Trust?



Two architectures, opposite trust models

- **Screen scraping** required the customer to hand their bank password to a third party. The TPP logged in impersonating the customer. The bank could not distinguish the customer from the scraper. No consent mechanism, no audit trail, no regulation.
- **Secure APIs** use token-based authorization (OAuth 2.0). The customer authenticates directly with the bank via SCA. The TPP receives a limited-scope token – never the password. Every access is logged and auditable.

Why screen scraping persisted

APIs are better in every way – so why did scraping survive for years? Because banks had no incentive to build APIs. Sharing data helps competitors. PSD2 forced the issue: banks **must** provide APIs. Scraping is now a fallback, not the norm.

Screen scraping required handing your password to a stranger – APIs replaced this with token-based access where the bank stays in control of authentication.

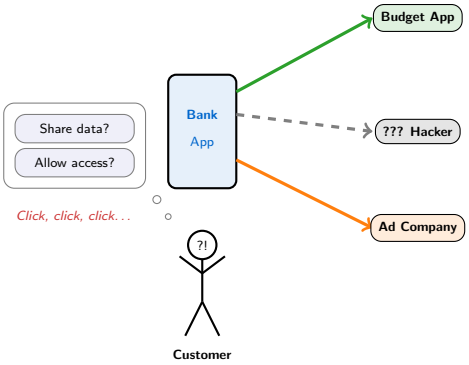
What Happens When Your Financial Data Leaks?

The Paradox of Openness
Open banking creates value by sharing data. But every new connection is a new attack surface. The more parties that access your financial data, the greater the risk of breach, misuse, or manipulation.

What could go wrong:

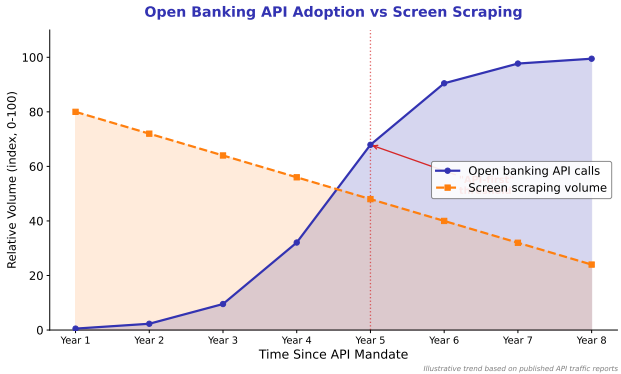
- **Consent fatigue:** Users click "agree" without reading – granting broad data access to apps they barely use. Studies show fewer than 10% read consent screens fully.
- **Third-party breaches:** A TPP with weak security becomes the weakest link. The bank's vault is secure, but the app that reads it may not be.
- **Data aggregation risk:** Combining transaction data from multiple banks creates a complete financial profile – valuable to hackers, advertisers, and hostile actors.
- **Zombie permissions:** Consent granted and forgotten. The 90-day re-authentication rule exists precisely because customers forget who has access.

The fundamental tension: Data sharing enables innovation. Data sharing also enables exploitation. The difference is the strength of the consent model.



More doors open means more doors to guard – the promise of open banking only works if consent is meaningful and security is real.

How Fast Are Open Banking APIs Replacing Screen Scraping?



Two curves, one crossover

- **API calls are surging:** Open banking API traffic has grown exponentially since mandated access took effect, following a hockey-stick adoption curve
- **Screen scraping is declining:** As APIs become available and reliable, scraping volumes fall – but have not reached zero
- **The crossover point:** The moment when API calls first exceed scraping marks the "API-first" threshold – the industry's point of no return

What drives API adoption?

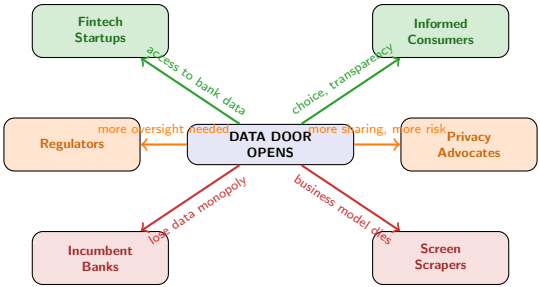
- Regulatory mandates (PSD2 in EU, Open Banking in UK)
- Developer ecosystem growth (fintech startups)
- Improved bank API quality over time
- Consumer awareness and trust building gradually

Why scraping persists:

- Some markets lack API mandates (parts of US, Asia)
- Bank API quality varies – compliance-minimum
- Legacy integrations not yet migrated

Illustrative trend based on published API traffic reports. The crossover point – where API calls exceed screen scraping – marks the shift from old world to new.

Who Wins and Who Loses When Banks Must Open Their Vaults?



Winners

+ **Fintech startups:** Can now build products on bank data without needing a banking license. Account aggregation, credit scoring, and payment initiation become viable businesses.
+ **Informed consumers:** More choice, better tools, lower fees from increased competition. Those who actively manage consent benefit most.

Losers

– **Incumbent banks:** Lose the data monopoly that protected their customer relationships. Must now compete on service quality, not data lock-in.
– **Screen scraping firms:** Their business model – scraping data without regulation – is replaced by the very APIs that make them obsolete.

Mixed impact

~ **Regulators:** Achieved the goal of more competition but must now supervise a much larger ecosystem of TPPs.
~ **Privacy advocates:** Data portability empowers customers but also normalizes data sharing – a double-edged sword.

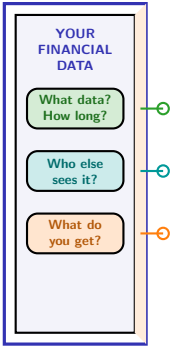
Open banking redistributes power from data hoarders to data users – but the biggest beneficiaries may not be customers.

The Consent Paradox: 3 Questions to Ask Before Sharing Your Data

The Open Banking Consent Checklist
Before granting any app access to your bank data, ask:

1. **What data, and for how long?**
   Does the app need your full transaction history, or just your balance? Is consent time-limited (90 days under PSD2) or indefinite? Can you revoke access instantly?
2. **Who else sees it?**
   Does the TPP share your data with fourth parties – advertisers, credit agencies, data brokers? Read the privacy policy, not just the consent screen.
3. **What is the value exchange?**
   What do you get in return for sharing your data? A genuinely useful service (budgeting, cheaper credit)? Or is your data the product being sold?

The consent paradox: Open banking only works if customers share data. But rational customers would share as little as possible. The system depends on a level of trust that consent fatigue undermines.



Three locks to check before you open the door.

Consent is only meaningful if you understand what you are consenting to – these three questions turn a click into a decision.

Your Challenge: Map the Data Flows Behind a Financial App

Mini-Challenge (15 minutes)

Choose **one** financial app you actually use – a budgeting tool, a payment app, or a trading platform. Investigate what data it accesses from your bank account and how.

Your deliverable: A one-page data flow map with three sections:

1. **Data flow diagram:** Draw the path your data takes. Start at your bank account. Show each intermediary (API gateway, TPP servers, analytics). End at the app screen you see. Label each arrow with what data moves.
2. **Consent audit:** Apply the three-question checklist from the previous slide:
   - What data does the app access, and for how long?
   - Does it share your data with fourth parties?
   - What value do you receive in exchange for your data?
3. **Trust verdict:** Based on your analysis, rate the app's data practices on a three-point scale:
   - $+$ **Trustworthy:** Clear consent, limited data, obvious value
   - $\sim$ **Questionable:** Broad access, unclear sharing, mixed value
   - $-$ **Concerning:** Excessive data, opaque sharing, data is the product

Conclude with one sentence: Would you continue using this app knowing what you now know about its data practices?

The best way to understand data sharing is to trace it yourself – pick an app, follow the data, and decide whether the trade-off is worth it.