Open Banking: Who Should Control Your Financial Data?

Banks used to own your data because they owned the vault – APIs pried the vault open, and now everyone wants a key

Digital Finance

Why Did It Take a Law to Make Banks Share Your Own Financial Data?

The Incentive Problem

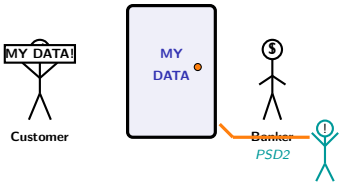
Banks had no reason to share your data. Your transaction history is a competitive moat – it predicts your behavior, locks you in, and makes switching expensive. Sharing it voluntarily would be like a fortress handing out keys.

Before PSD2 (January 2018):

- Third-party apps used **screen scraping** – logging in as you, parsing HTML, extracting data from web pages
- Banks could block scrapers without consequence
- No standardized data format, no audit trail, no consent framework
- Customers had no legal right to machine-readable data portability

After PSD2:

- Banks **must** provide standardized APIs to licensed third parties
- Customer consent is explicit, granular, and time-limited (90 days)
- Strong Customer Authentication (SCA) protects every access
- A new regulatory category – Third-Party Providers (TPPs) – was born



Banks accumulated decades of customer data with no obligation to share it – PSD2 created a legal right to data portability that no market force had delivered.

How Many Third-Party Apps Can See Your Bank Balance Right Now?

Reflection Prompt

Open your phone's settings and look for "connected accounts" or "linked services." Count every app that has access to your bank account – budgeting tools, payment apps, investment platforms, buy-now-pay-later services.

For each one, answer three questions: What data can it see? When did you grant access? Can you revoke it right now?

Most people cannot answer any of these questions. They clicked "Allow" months ago and never thought about it again. This is the consent problem at the heart of open banking.

The exercise reveals three uncomfortable truths:

- You probably granted more access than you remember
- You almost certainly did not read what data each app can see
- You may not know how to revoke access if you wanted to
- Some of these connections may still use screen scraping, not secure APIs

Open banking was designed to give you control. But control requires awareness – and awareness requires effort that most people never invest.

Bring your count to class. We will use it as a baseline when we discuss the consent funnel on Slide 6.

The gap between "you have the right to control your data" and "you actually exercise that right" is the central tension of open banking.

What Can a Third-Party App Actually Do With Your Bank Account?

Dimension	AISP	PISP	CISP
Full name	Account Information Service Provider	Payment Initiation Service Provider	Card-Based Payment Instrument Issuer
What it does	Reads account data (balances, history)	Initiates payments from your account	Issues cards linked to your account
Data flow	Read-only	Write (payment order)	Read (balance check)
Example	Budgeting app aggregating 3 banks	Klarna checkout bypassing card network	Virtual card issued by fintech
SCA required	Yes (every 90 days)	Yes (per transaction)	Yes (per issuance)
Key risk	Data aggregation, profiling	Unauthorized payment if consent weak	Card fraud if issuance controls weak

The critical distinction: AISPs can only **read** your data. PISPs can **move your money**. CISPs can **issue instruments** that spend your money. Each requires a different license and different levels of regulatory oversight.

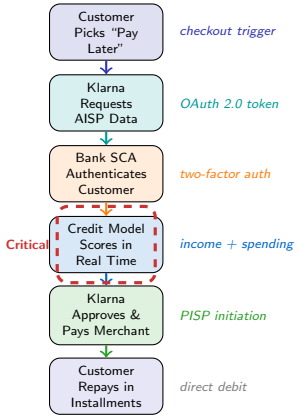
Three types, three risk profiles

- **AISP (read):** The lowest risk category. The app can see your transactions and balances but cannot move a cent. Risk is privacy, not theft.
- **PISP (write):** The app can initiate a payment directly from your bank account – bypassing card networks entirely. Risk is unauthorized transactions if the consent model is weak.
- **CISP (issue):** The app can create a payment card linked to your account. Every transaction on that card draws from your balance. Risk is fraud if card controls are insufficient.

Layering matters: A single fintech can hold all three licenses. Klarna, for example, reads your data (AISP) to assess credit, initiates payment (PISP) at checkout, and could issue a virtual card (CISP) – all in one flow.

PSD2 created three distinct TPP categories – each with different capabilities, different risks, and different regulatory requirements.

Follow One Klarna "Pay Later" Transaction Through the Open Banking Stack



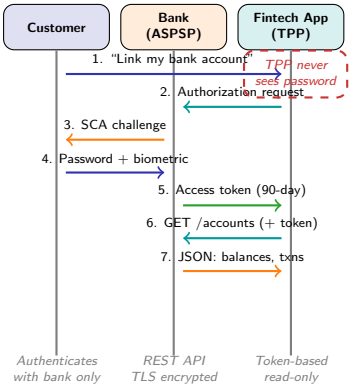
Six steps, two API types, zero passwords shared

- **Checkout trigger:** The customer selects "Pay in 3" at an online merchant. Klarna (Sweden, Stockholm, 2005, BNPL market leader, CEO Sebastian Siemiatkowski, licensed Swedish bank since 2017) needs to assess credit risk instantly – no time for a traditional credit check.
- **AISP request:** Klarna uses its AISP license to request the customer's recent transaction history from their bank via API. This reveals income regularity, spending patterns, and existing commitments.
- **Bank authentication:** The customer authenticates directly with their bank via SCA. Klarna never sees the bank password – only a time-limited OAuth token.
- **Credit scoring:** Klarna's ML model processes the transaction data in real time. Approval or rejection happens in seconds, not days.
- **Payment:** Klarna pays the merchant immediately using its PISP license to initiate a payment from its own funds. The merchant gets paid; the customer owes Klarna.
- **Repayment:** The customer repays in installments. Klarna profits from merchant fees and late payment charges.

Key insight: Open banking APIs turned a credit decision from a days-long process into a seconds-long one.

One Klarna checkout uses two PSD2 API types (AISP + PISP), one OAuth flow, one SCA step, and one ML model – all invisible to the customer.

How Does a Third-Party App Talk to Your Bank Without Knowing Your Password?



OAuth 2.0: the security backbone
The entire open banking security model rests on one principle: the customer authenticates with the **bank**, never with the third party.

- **ASPSP = Account Servicing Payment Service Provider:** the bank whose account a customer holds. Under PSD2, every ASPSP must expose standardised APIs to licensed TPPs.
- **REST API:** Communication uses standard HTTP methods (GET, POST) with JSON payloads. Every European bank must expose at least account and transaction endpoints.
- **OAuth 2.0:** The authorization framework. The bank issues a time-limited access token. The TPP presents this token with every API call – never a password.
- **SCA:** Strong Customer Authentication requires two of three factors – something you know (PIN), something you have (phone), something you are (fingerprint).
- **TLS encryption:** All data in transit is encrypted. The TPP cannot intercept data between the customer and the bank.
- **90-day expiry:** Tokens expire. The customer must re-authenticate periodically, preventing zombie permissions.

The architecture insight: Open banking separated *authentication* (proving identity) from *authorization* (granting access). The bank handles the first; the token handles the second.

OAuth 2.0 solved the fundamental problem of screen scraping: how to share data without sharing passwords.

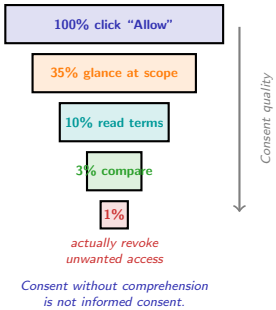
What Happens When Consent Becomes a Checkbox No One Reads?

The Consent Funnel Problem
Open banking was designed around informed consent. In practice, consent has become a speed bump that users click through as fast as possible.

The three consent failures:

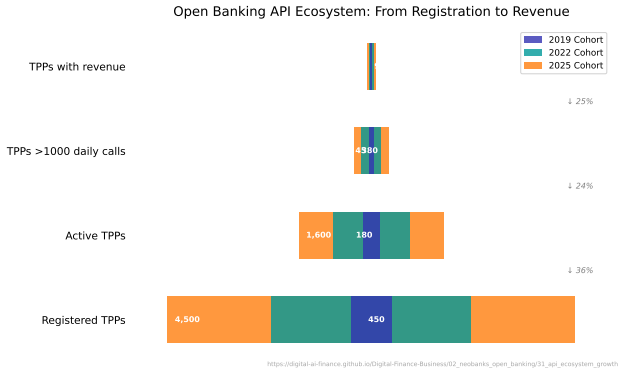
- **Consent fatigue:** Users encounter dozens of permission requests per week. Studies show fewer than 10% read consent screens fully. The rest click "Allow" reflexively.
- **Data aggregation risk:** A single AISP may connect to three banks. Combined, it builds a complete financial profile – income, spending, debts, investments – more detailed than any single bank holds.
- **Screen scraping persistence:** In markets without mandatory APIs (parts of the US, Asia-Pacific), third parties still request bank passwords directly. PSD2 banned this in Europe, but compliance is uneven.

The paradox: The more granular consent becomes (per-account, per-data-type, per-purpose), the more consent screens users face – and the less likely they are to read any of them.



Illustrative estimates based on published consent-behavior research. The consent funnel narrows dramatically – most open banking permissions are granted without genuine understanding.

How Fast Is the Open Banking API Ecosystem Growing?



What the growth trajectory reveals

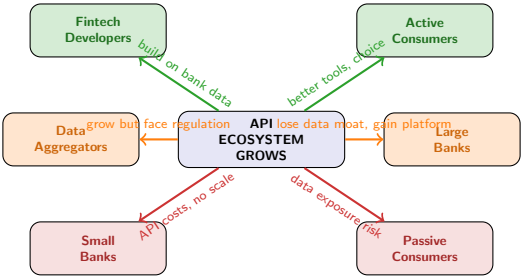
- **API endpoints are multiplying:** Banks are moving beyond compliance-minimum APIs to richer offerings – account data, payment initiation, identity verification, and product comparison endpoints
- **TPP registrations are accelerating:** The number of licensed AISPs and PISPs in Europe has grown steadily since PSD2 took effect, indicating sustained developer interest
- **API call volumes follow a hockey stick:** Early adoption was slow as banks built minimum-viable APIs, but once quality improved, usage surged
- **Premium APIs are emerging:** Some banks now offer paid API tiers with richer data, faster response times, and dedicated support – turning compliance into revenue

The regional gap:

- UK leads (Open Banking Implementation Entity = OBIE, UK, set up Sep 2016 by the Competition and Markets Authority)
- EU follows (PSD2 mandated but fragmented across 27 markets)
- US lags (no federal mandate; CFPB Rule 1033 = Consumer Financial Protection Bureau personal-financial-data right, final rule Oct 2024)
- Asia-Pacific mixed (Singapore SGFinDex launched 2020 by MAS; Australia Consumer Data Right active Jul 2020; others not)

Illustrative trend based on published API adoption data. The ecosystem is growing, but quality and coverage remain uneven across markets.

Who Wins and Who Loses When APIs Replace Proprietary Bank Channels?



Winners

+ **Fintech developers:** Can build products on standardized bank data without a banking license. API access lowers the barrier to entry for financial innovation.
+ **Active consumers:** Those who engage with consent controls get better budgeting, cheaper credit, and consolidated financial views.

Losers

– **Small banks:** Must build expensive APIs to comply with PSD2 but lack the scale to monetize them. Compliance is a fixed cost on a small base.
– **Passive consumers:** Those who click "Allow" without reading face data aggregation and profiling risks they never consented to meaningfully.

Mixed impact

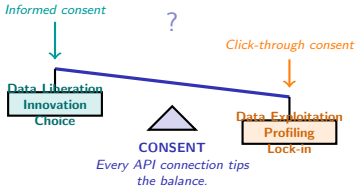
~ **Data aggregators:** Grow rapidly (market leaders: Plaid, US, 2013, $13bn valuation; Tink, Sweden 2012, acquired by Visa Mar 2022 ~$2bn; TrueLayer, UK 2016; Yodlee, US 1999 pioneer) but face increasing regulatory scrutiny under proposed open finance rules.
~ **Large banks:** Lose the data monopoly but can reinvent themselves as API platforms – selling data access as a service.

The API economy creates asymmetric outcomes – active consumers and skilled developers benefit most, while small banks and passive users bear disproportionate costs.

Four Questions to Ask Before Granting Any App Access to Your Bank

The Open Banking Due Diligence Checklist
Before any financial app connects to your bank account, ask:

1. **What is the minimum data it needs?**
   Does the app need your full transaction history, or just your current balance? A budgeting app needs transactions. A "Pay Later" service only needs recent income. If it asks for everything, ask why.
2. **Can you revoke access in one click?**
   Check whether your bank provides a consent dashboard where you can see and revoke all active TPP connections instantly. If revoking requires contacting the TPP, the power balance is wrong.
3. **Where does your data go after the app receives it?**
   Does the TPP store your data locally? Share it with fourth parties (advertisers, credit agencies, analytics firms)? The privacy policy – not the consent screen – reveals this.
4. **What happens if the provider disappears?**
   If the fintech shuts down, who holds your data? Is it deleted automatically? Or does it persist on servers with no ongoing security maintenance?



These four questions turn a reflexive click into a deliberate decision – the difference between data liberation and data exploitation.

Should Open Finance Extend Beyond Banking to Insurance, Pensions, and Investments?

Mini-Challenge (15 minutes)

The EU is proposing the **Financial Data Access Regulation (FIDA)** – proposed by the European Commission in June 2023, currently in trilogue negotiations – extending PSD2-style API access beyond bank accounts to insurance policies, pension funds, and investment portfolios. A single app could show your complete financial life: bank balances, insurance coverage, pension projections, and investment performance.

Apply the four due diligence questions to this proposal:

1. **What is the minimum data needed?**
   - Does a budgeting app need your pension projections?
   - Does a robo-advisor need your insurance claims history?
   - Where is the line between "useful aggregation" and "excessive profiling"?
2. **Can you revoke access in one click?**
   - Today you cannot revoke bank API access easily. Will insurance/pension APIs make consent management even harder?
3. **Where does the data go?**
   - A combined financial profile is worth far more to data brokers than bank data alone. Who benefits from that aggregation?
4. **What if the provider disappears?**
   - With full financial profiles at stake, a fintech shutdown becomes a data breach waiting to happen.

Closing thought: Open banking gave you data freedom. Nobody mentioned the consent paperwork.

Open finance is the next frontier – but every extension of API access multiplies both the opportunity for innovation and the surface area for exploitation.