



A Fair Exchange: Why Data Aggregators Should Pay to Access Bank APIs

July 17, 2025

The banking sector is investing heavily in digital infrastructure and technological capabilities to expand the products and services available to customers and to increase the speed, safety and efficiency of modern banking. A [McKinsey](#) study found that banks spend about \$650 billion per year on IT, or about 6-12% of total annual revenue. That's nearly double the amount spent by other industries, such as telecommunications and media.

These investments help power a wide range of services, such as mobile banking and peer-to-peer payments. They also contribute to the development of secure data-sharing systems and application programming interfaces (APIs) so consumers can securely connect their bank accounts to third-party financial apps and services of their choosing. These connections are sometimes made through direct partnerships between a bank and a fintech; other times, these arrangements are enabled by middlemen called data aggregators. More than 120 data aggregators operate in the U.S. today, securely linking [hundreds of millions](#) of bank accounts across providers with fintechs.

Certain fintechs and data aggregators object to paying access fees for consumer data sharing APIs. These criticisms ignore the substantial costs associated with building and maintaining systems to provide secure data-sharing services and contradict standard business practices relied on by data aggregators themselves when facilitating data transfers. The criticisms also ignore the nature of what's actually happening: this isn't about a customer exporting transaction history or account records, a routine, low-cost interaction. It's about high-volume, often continuous data extraction by data middlemen, frequently without the customer's awareness, with the intent to store and resell the financial data.¹

Data-Sharing Agreements Have Enabled the Current Ecosystem to Thrive

Data-sharing agreements govern relationships between banks and data middlemen and have made today's thriving U.S. data-sharing ecosystem possible. These agreements are made in advance of data sharing by banks and fintechs to mitigate potential issues and address unsafe data-collection practices like [screen scraping](#). They establish the terms and conditions of the arrangement, including how the data is used, how long it is saved, how it is protected and who is liable to the customer if that data is misused. Data-sharing agreements also outline the commercial terms between companies, including any fees that data middlemen must pay to access consumer data securely.

Banks must follow strict regulatory timelines for retaining and deleting consumer data, yet aggregators often keep the same data indefinitely unless the contract mandates timely deletion. In many cases, consumers may not realize how frequently their data is accessed. [Unbeknownst to the consumer](#), what looks like a one-time connection may be a near-constant data extraction behind the scenes.

¹ See "Fintechs Want to Protect Data-Sharing Privileges, Just Not for Consumers" (<https://bpi.com/fintechs-want-to-protect-data-sharing-privileges-just-not-for-consumers/>).

Fintechs and Aggregators Generate the Overwhelming Majority of Data Requests

Aggregators typically operate their businesses by obtaining data from banks, saving that data into their own systems and selling access to fintech developers building financial applications. Fintechs and aggregators generate the majority of data requests, and this type of commercial activity generates significant commercial value for these middlemen while draining bank resources and introducing data security risks that may expose the banks to increased liability for those risks.

The largest aggregator is currently Plaid, which connects to more than [200 million](#) bank accounts. Fintechs leverage these services to offer cash flow monitoring, payment authentication and a variety of other products and services that rely on consumer financial data.

API-Based Pricing

Like many technology firms, data aggregators often charge fintechs and other clients based on the volume of API calls. An API call occurs when one application requests data from another. For example, a budgeting app might make an API call to a user's bank to update their account balance after a paycheck is deposited. Aggregators act as the conduit in that exchange, helping the two applications communicate securely and reliably.

Companies that charge businesses based on API calls often rely on tiered pricing structures to cover some of these expenses. Charging for API access is standard for almost every major company, including [Amazon Web Services](#), [Microsoft Azure](#), [X](#) (formerly known as Twitter), [Google](#), and others.

API Limits

Every API call is a new request that a bank's data server must receive and process, and those calls place a demand on those servers. Banks and technology companies address this by imposing [API limits](#) to manage call volume to prevent data servers from becoming overwhelmed.

Think of it like a bank call center. Eventually, the bank will run out of available call operators and will either need to place calls on hold (similar to an API limit) or invest in additional staffing and infrastructure to accommodate higher volumes. The same principles apply to data sharing.

These limits help banks manage demand. They also encourage fintechs and other API users to evaluate how often they truly need access to certain information. For example, the same budgeting app referenced earlier using an API to obtain a customer account balance likely doesn't need to refresh that data (i.e., issue a new API call) instantly; updating it occasionally may be sufficient.

API limits and fees imposed on API call volume help companies manage volume and business-related expenses while providing the best possible service for their customers. While there is no publicly available data in the U.S., [data](#) from the U.K. open banking program show that there were 1.99 billion API calls in May 2025 alone. According to [Qwist](#), third-party providers, not banks, generate 96 percent of open banking API calls in Europe. Many of these requests originate from a small group of large data aggregators.

The Bottom Line: Charging Data Middlemen Helps Banks Cover Business Expenses

Banks have a strong track record of partnering with fintechs and safely sharing customer data. But data sharing comes at a cost. Charging data middlemen responsible for the largest volume of requests allows banks to cover basic business expenses without passing those costs onto consumers.

These fees help cover infrastructure, utility costs, staffing, cybersecurity, data security controls and enhancements necessary to maintain the quality and reliability of these systems. They also encourage more responsible and efficient data-gathering practices from aggregators, minimizing the amount of sensitive consumer financial data in circulation. Ultimately, banks' ability to negotiate pricing with aggregators and other data middlemen helps maintain a competitive and secure financial system.