Payments System Research Briefing

Open Banking: A Critical Piece in the Future of Financial Services

By Julian Alcazar and Sam Baird

Open banking enables consumers to securely share data from their bank accounts with third-party service providers. By using application programming interfaces, open banking facilitates innovations such as Pay-by-Bank payments, instant bill payments, and cash-flow-based lending. While regulatory efforts are underway at both federal and state levels, technological and operational barriers and a lack of standardization continue to challenge widespread use of open banking in the United States.

U.S. consumers increasingly rely on real-time access to data from their bank accounts to manage their finances via services or apps offered by third-party service providers (TSPs). However, sharing this financial data with TSPs is not straightforward and may involve risks and delays. Open banking may allow easier data sharing between financial institutions and TSPs, enabling more innovative products and services. However, implementing an open banking framework in the United States may pose challenges. In this *Payments System Research Briefing,* we provide an overview of open banking, discuss the ways it may enable financial services innovation, and highlight the potential barriers it faces to widespread use in the United States.

What is open banking?

Open banking is a financial services model that allows consumers to share data from their bank accounts—such as account balances and transaction history—with TSPs, including other banks and fintech apps. Consumer-permitted financial data flow from banks (and credit unions) to TSPs through application programming interfaces (APIs), facilitated by data aggregators. In a typical open banking data flow, (1) the consumer authorizes the TSP to access their financial data, (2) the TSP communicates with the data aggregator through an API to request data from the consumer's bank, (3) the data aggregator communicates with the consumer's bank to extract the data through another API, and (4) the data aggregator forwards the data to the TSP through the same API used in (2). Based on the data extracted, the TSP provides a service to the consumer (Alcazar and Hayashi 2022).

Open banking is more secure, efficient, and timely than other data extracting methods, such as screen scraping. Screen scraping involves consumers sharing their financial account credentials with a TSP, allowing the TSP to log in to their account to extract data. Although screen scraping has been a common method of data extraction, it is prone to exposing consumers' account credentials to bad actors, as consumers may need to share their credentials with multiple TSPs. In addition, a consumer's bank may not be able to easily decipher whether the accountholder, an authorized TSP, or a bad actor is logging in to the account. In contrast, with open banking, consumers' account credentials are shared only with a small number of data aggregators, and APIs enable banks to act as gatekeepers, controlling the amount and type of data consumers share. Moreover, APIs locate data more efficiently than screen scrapers and allow real-time data access across multiple financial accounts, enabling TSPs to use a consumer's most accurate and up-to-date financial information to provide services.

Open banking and financial service innovations

By giving TSPs the ability to access financial data of a consumer instantaneously with fewer resources than other data extracting methods, open banking allows TSPs to offer innovative financial services. One service made possible with open banking is Pay-by-Bank, also known as account-to-account or bank account-based payment. In a transaction with Pay-by-Bank, the consumer makes a payment by directly transferring funds from their bank account to the merchant's bank account via an Automated Clearing House (ACH) network or an instant payment network. In a Pay-by-Bank payment, open banking establishes a connection between the merchant (or their service provider) and the consumer's bank via the consumer's online or mobile banking app. At the online or physical checkout, the consumer's app receives the merchant's bank account information, and the consumer approves a funds transfer within their app. This process reduces the friction of payment authorization, as it does not require manually entering checking or card account details. When paired with instant payments, Pay-by-Bank enables real-time funds transfers, allowing merchants to receive funds instantaneously instead of up to a few days later due to ACH's batch processing.

Another service, Request for Payment (RfP), combines open banking's API-driven data sharing with instant payments to allow consumers to pay bills instantly. Instant payment networks offer RfP to allow billers to send secure, real-time payment requests to their customers. Because the RfP includes the biller's bank account details, the customer makes a bill payment instantly by simply responding to the RfP. RfP may reduce erroneous payments; without it, the customer may need to input the biller's bank account details themselves, introducing greater potential for error. RfP may also reduce failed payments and fees a customer might incur due to insufficient funds. By responding to the RfP, the customer explicitly approves their bank to initiate the payment. The bank verifies in real time that sufficient funds are available before processing the transaction, thereby preventing a failed payment that would otherwise result in an insufficient funds fee.

In addition to payment services, open banking may also facilitate innovation in credit underwriting and fraud mitigation. For example, open banking enables loan services using cash flow underwriting. Through open banking, a potential lender could use a borrower's transaction history (such as income deposits, recurring expenses, and payment patterns) as an alternative or in addition to traditional credit data to assess their creditworthiness and determine loan terms. Using this alternative or additional data in credit underwriting may expand credit access for consumers with no or limited credit histories (Toh 2023). More generally, open banking enables financial services to better mitigate fraud. Because open banking allows a consumer-authorized TSP to access up-to-date account information, the TSP can verify account ownership, check balances, and assess behavioral patterns before initiating a financial transaction. These activities help reduce risks of fraudulent financial transactions involving identity theft, synthetic identities, and account takeovers.

Efforts to regulate open banking in the United States

The lack of a regulatory framework for open banking has delayed wider implementation of open banking in the United States relative to other countries. Although Section 1033 of the Dodd-Frank Act (enacted in 2010) grants consumers the right to access information about the financial products and services they use and direct that information to third parties, the rule enforcing 1033 has yet to be implemented

(Congressional Research Service 2023). In October 2024, the Consumer Financial Protection Bureau (CFPB) finalized the Personal Financial Data Rights (PFDR) rule, but banking trade associations filed a lawsuit to challenge the rule (Federal Register 2024). The CFPB vacated the rule in May 2025 and requested a stay, which was granted by the court in July 2025. In August 2025, the CFPB released advanced notice on PFDR reconsideration, but CFPB has not released the new, revised rule as of this writing.

In general, the PFDR rule requires financial institutions, or "data providers," to provide covered data (including information about transactions, costs, charges, and usage) to consumers and authorized TSPs upon request. The rule applies to financial institutions that hold transaction accounts, including credit card accounts, or that provide other types of payment facilitation products or services. The rule also contains provisions regulating how covered data are to be made available and accessed as well as provisions establishing authorization procedures and obligations for TSPs. Some of the provisions currently being reconsidered include the fees that data providers may charge to consumers to access their data. Other provisions under review relate to information security, including methods of data access (such as APIs and screen scraping), information security standards, and data providers' denying access to covered data due to information security risks (Federal Register 2025).

While the industry waits for the CFPB to rework the PFDR rule at the federal level, legislation governing open banking has been developed at the state level. In March 2026, New York lawmakers proposed the first two pieces of legislation (A10540 and S9483) to govern open banking. This legislation would provide consumers the right to access their data, prohibit banks from charging fees for access to covered data, require banks to establish developer interface-based access to consumer financial data, and set security standards for authenticating users.[1] The legislation defines covered banks as any New York state bank and any entity that provides a financial product or service for New York residents (including out-of-state banks, trusts, or data providers). Under this legislation, the New York Department of Financial Services would be granted enforcement powers to impose civil penalties for infractions up to $10,000.

Although future federal regulation may preempt state law, if New York's proposed legislation were passed and enacted before the CFPB finishes the PFDR rework, it could have significant near-term implications. New York is uniquely influential in the open banking landscape because many banks and TSPs serve residents in the state. Even if banks and TSPs do not currently operate in New York, open banking practices that comply with New York's legislation could be adopted as common practices among institutions nationwide.[2]

Barriers to open banking for financial institutions

In addition to the lack of a regulatory framework for open banking, significant technological and operational hurdles for financial institutions have kept open banking from proliferating widely in the United States. The regulations governing open banking may require banks and credit unions to establish secure, reliable electronic interfaces to enable data exchanges among parties, but the industry participants determine how such interfaces must be established. For consumer-permitted data to move securely and reliably across the open banking ecosystem, it is critical for the industry to create

interoperable frameworks involving set standards for data schemas, authentication protocols, and API formats and performance baselines.

The absence of universally accepted standards contributes to market fragmentation, delaying open banking implementation. For example, financial institutions and TSPs currently use numerous slightly different API formats, requiring data aggregators to support various formats, and financial institutions, as data providers, to navigate inconsistent implementation guidance from vendors. Industry groups such as the Financial Data Exchange (FDX) are working to define API format common specifications, but so far, adoption remains uneven (FDX 2026). Without stronger alignment around standards, open banking risks evolving into a patchwork of incompatible approaches rather than a cohesive, interoperable framework.

Beyond the challenge of market fragmentation, financial institutions face substantial technological and operational demands in implementing open banking. Technologically, financial institutions must invest in modernizing their internal systems and standardizing databases. Many institutions still rely on outdated core banking systems that were not designed to support real-time data retrieval, high-throughput API calls, or the event-driven architecture required for modern open banking frameworks.[3] Internal data silos, inconsistent data labeling, and legacy middleware layers—that is, software sitting between internal systems that help the systems exchange data—further complicate API deployment. Operationally, financial institutions must redesign internal workflows to manage third-party access, ongoing consumer authorization, and enhanced security monitoring. These enhancements will require implementing dedicated API management platforms, conducting continuous uptime monitoring, establishing consumer consent dashboards, and training staff on emerging fraud patterns associated with real-time payments and data sharing.

Most community banks and credit unions rely heavily on core banking services providers to develop these technological and operational capabilities, as doing so internally may be cost prohibitive (Alcazar and others 2024a, 2024b). As a result, core services providers' modernization roadmaps may significantly affect the pace at which community banks and credit unions can implement open banking. A few legacy core services providers have sizable market share in the core services market; if these providers are slow to offer necessary services for open banking, community banks and credit unions risk falling behind in the open banking transition (Alcazar and others 2024c). Next-generation core providers' entrance into the market, however, may place competitive pressure on incumbents to accelerate the transition.

Conclusion

Open banking is an important framework for modernizing data sharing between consumers' financial institutions and TSPs and enabling opportunities for innovative products and services. Regulatory bodies such as the CFPB and the State of New York have proposed regulatory frameworks to enable open banking, but these efforts are still underway. How open banking evolves and facilitates financial services innovation in the United States may become clearer when the CFPB announces the rework of the PFDR rule.

Endnotes

[1] New York's S9483 would also provide small businesses with the right to access their financial data (New York State Senate 2026).

[2] Examples of state legislation that have provoked a nationwide response are California's data privacy laws, the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), which amended and significantly strengthened the CCPA. These laws set strict guidelines on a consumer's right to know, permit the use of, and request deletion of their data. In 2025, the California Privacy Protection Agency issued a $1.35 million fine to Tractor Supply Company, a Tennessee based company, for violating the CCPA and required the company to change business practices to comply with the laws (California Privacy Protection Agency 2025). New York's open banking legislation may require out-of-state financial institutions to change business practices in a similar fashion.

[3] Event-driven architecture refers to systems that process and share information the moment something changes (such as a balance update or new transaction), rather than waiting for scheduled updates.

References

Alcazar, Julian, Sam Baird, Emma Cronenweth, Fumiko Hayashi, and Ken Isaacson. 2024a. "Core Banking Systems and Options for Modernization." Federal Reserve Bank of Kansas City, *Payments System Research Briefing*, February 28.

Alcazar, Julian, Sam Baird, Emma Cronenweth, Fumiko Hayashi, and Ken Isaacson. 2024b. "The Role of Core Banking Services Providers in Facilitating Instant Payments." Federal Reserve Bank of Kansas City, *Payments System Research Briefing*, May 8.

Alcazar, Julian, Sam Baird, Emma Cronenweth, Fumiko Hayashi, and Ken Isaacson. 2024c. "Market Structure of Core Banking Services Providers." Federal Reserve Bank of Kansas City, *Payments System Research Briefing*, March 27.

Alcazar, Julian, and Fumiko Hayashi. 2022. "Data Aggregators: The Connective Tissue for Open Banking." Federal Reserve Bank of Kansas City, *Payments System Research Briefing*, August 24.

California Privacy Protection Agency. 2025. "Nation's Largest Rural Lifestyle Retailer to Pay $1.35M Over CCPA Violations." *News*, September 30.

Congressional Research Service. 2023. "CFPB Proposes New Regulation on Consumer Data Rights." December 19.

FDX (Financial Data Exchange). 2026. "About FDX: Our Mission."

Federal Register. 2025. "Personal Financial Data Rights Reconsideration." August 22.

Federal Register. 2024. "Required Rulemaking on Personal Financial Data Rights." November 18.

New York State Senate. 2026. "Senate Bill S9483."

Toh, Ying Lei. 2023. "Addressing Traditional Credit Scores as a Barrier to Accessing Affordable Credit." Federal Reserve Bank of Kansas City, *Economic Review*, vol. 108, no. 3.

Julian Alcazar is a senior payments specialist at the Federal Reserve Bank of Kansas City. Sam Baird is an experienced payments specialist at the bank. The views expressed are those of the authors and do not necessarily reflect the positions of the Federal Reserve Bank of Kansas City or the Federal Reserve System.

To receive email alerts for payments research and other KC Fed publications, visit https://www.kansascityfed.org/about-us/ealert/