kcFED Payments System Research Briefing

Data Aggregators: The Connective Tissue for Open Banking

By Julian Alcazar and Fumiko Hayashi

Open banking, which allows third-party financial apps to access consumer financial data electronically and securely, relies on data aggregators to establish connections with consumers' financial institutions and extract consumer data. Data aggregators are critical to enhancing consumer financial services and increasing competition—both among financial service providers and across payment methods. However, their role raises some concerns related to data security, data privacy, and competition.

U.S. consumers are increasingly using financial apps offered by fintechs or nonbank service providers to manage budgets, make payments, and apply for loans. Such apps are made possible by open banking, a practice of electronically and securely sharing financial data—with the consumer's approval—from the consumer's financial institution with a third-party service provider (TSP). In open banking, data aggregators such as Finicity, MX Technologies, and Plaid play a critical but not well understood role. This *Payments System Research Briefing* describes the role of data aggregators in open banking and examines implications for the financial services industry.

Open banking: A new, better way to share consumer financial data with TSPs

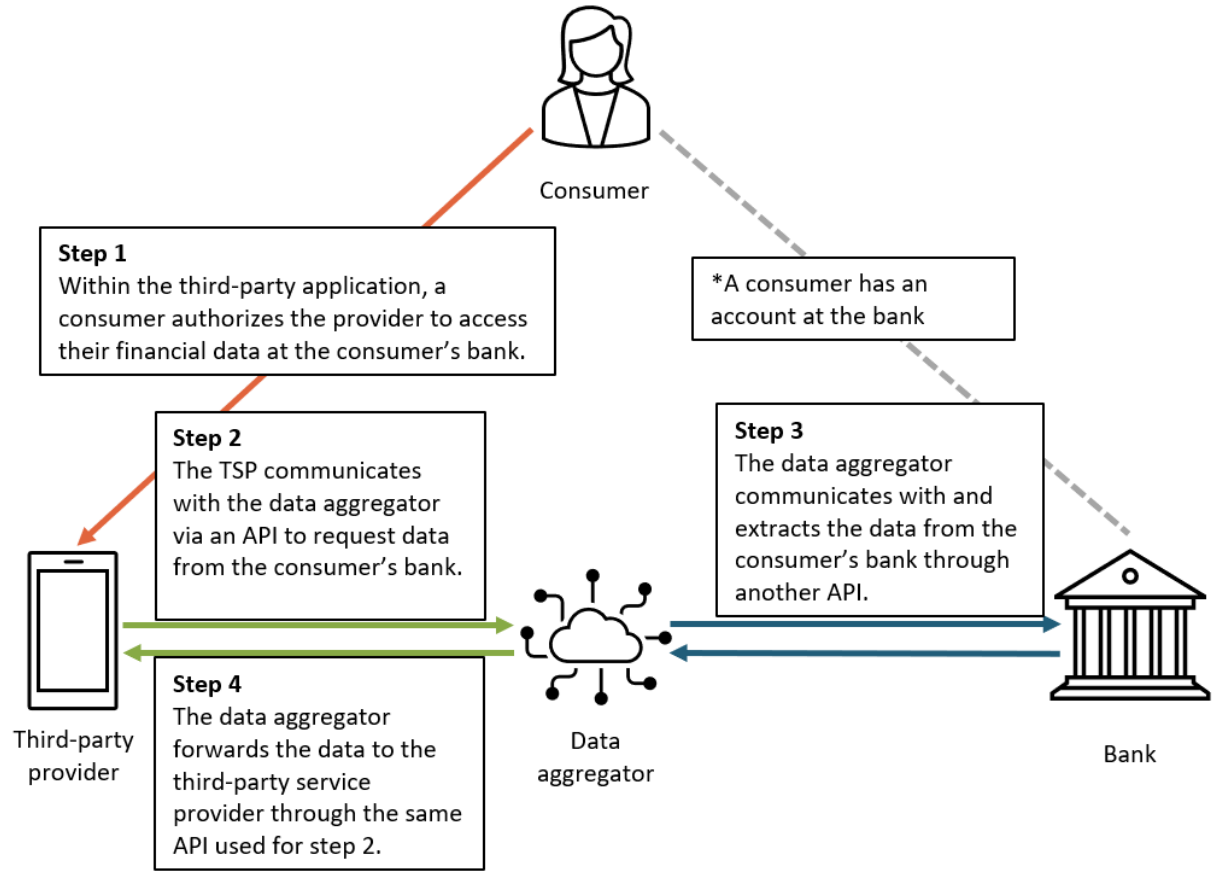
Prior to open banking, TSPs primarily accessed consumer financial data through "screen scraping." In this process, a consumer authorizes a TSP to log in to their bank account and extract data, often using a data aggregator to collect and package the data. However, screen scraping is not a secure practice. The consumer's bank cannot tell if the party logging in to the account is the accountholder, the consumer's authorized third party, or a fraudster, and consumers and their banks do not have control over the amount and type of information extracted from accounts (such as account number, routing number, account balance, and transaction history). A consumer's bank account credentials are also more likely to be exposed to bad actors, as each TSP that provides financial services to a consumer stores their account credentials. In addition, screen scraping is less efficient and may yield less timely data. Accessing a consumer's account requires time and resources, and consequently, TSPs extracted consumer data less often. As a result, the data often became obsolete by the time TSPs provided consumers services.

Compared with screen scraping, open banking is more secure, more efficient, and instantaneous. In open banking, consumer-permissioned financial data flow from their financial institutions to TSPs through application programming interfaces (APIs)—a set of defined rules that enable different software to communicate and exchange data. APIs allow consumers to share their financial data with TSPs without sharing their financial account credentials. Instead, their credentials are shared only with a small number of data aggregators, which extract consumer data on behalf of numerous TSPs. APIs also offer consumers the ability to control the amount and type of data they share, as their financial institutions act as gatekeepers. Moreover, APIs allow real-time data access using fewer resources than screen scraping, enabling TSPs to access consumer data in multiple accounts at various financial institutions and provide consumers services based on their current financial situation.

Data aggregators' role in open banking

In open banking, new-generation data aggregators that specialize in APIs, such as Finicity, MX, and Plaid, facilitate the API-based flow of data from consumers' financial institutions to TSPs. Figure 1 shows how a data aggregator connects a consumer-authorized TSP with the consumer's bank.[1] After the consumer authorizes the TSP to access their financial data (step 1), the TSP communicates with the data aggregator through an API to request data from the consumer's bank (step 2). The data aggregator then communicates with and extracts the data from the consumer's bank through another API (step 3). The data aggregator forwards the data to the TSP through the same API used for step 2 (step 4). Based on the data extracted, the TSP provides a service to the consumer.

Figure 1: A data aggregator connects a consumer-authorized TSP and the consumer's bank via APIs



New-generation data aggregators perform three distinct functions. First, they offer their own APIs that individual TSPs can use to build fintech apps to extract data from consumers' financial institutions, allowing consumers to seamlessly connect their financial accounts to the apps. Second, as illustrated in Figure 1, data aggregators serve as intermediaries between a consumer's financial institutions and authorized TSPs. Having several API connections with data aggregators enables thousands of financial institutions and numerous TSPs in the United States to share data. Data aggregators typically have bilateral data-sharing agreements with many large banks to access their customers' financial data via direct API connections. To access consumer financial data at smaller banks, data aggregators generally

partner with core banking service providers, which process daily banking transactions and post updates to customer accounts for those banks.[2] Third, after extracting consumer data from various financial institutions, data aggregators reformat the data and share them with TSPs. Because APIs used for accessing data at financial institutions have yet to be standardized in the United States, reformatting the data helps TSPs save resources and mitigate the risk of misinterpreting data.

How data aggregators can help enhance financial services

Data aggregators can help enhance consumer financial services in three main ways. First, data aggregators' connections with many financial institutions and ability to access a variety of consumer financial data can help improve personal financial management (PFM) tools used for budgeting, reducing debts, or preparing for retirement. For example, a data aggregator's API connections with numerous banks and other transaction account providers enable a PFM app to receive detailed transaction data from various accounts; the app can use these data to assist consumers with budgeting or maximizing their savings. In addition, a data aggregator's connections with various types of lenders, including credit card issuers and mortgage providers, enable a PFM app to receive data on a consumer's debt amounts and interest charges; the app can then use these data to provide consumers with tailored debt repayment advice, such as raising their monthly repayment or transferring credit card debts to a card with the lowest interest rate. A data aggregator's connections with institutions such as investment banks and retirement account providers also enable a PFM app to offer longer-term financial planning tools and advice.

Second, a data aggregator's ability to access a variety of consumer financial data can also help improve a consumer's loan application process and potentially increase their credit access. In the past, loan applications were cumbersome because they required information dispersed across consumers' various accounts; moreover, this information was submitted and reviewed in paper form. Today, data aggregators enable potential lenders (both nonbank lenders as well as financial institutions) to access a variety of consumer data electronically via APIs, making the loan application process less error prone and easier for both the consumer and lenders. Data aggregators also enable potential lenders to access consumer data that are not traditionally used for credit decisions, such as a consumer's good record of rent payments or other bill payments. These additional data may aid lenders in offering loans to consumers who have little or no credit history.

Third, a data aggregator's ability to access consumers' bank accounts at numerous banks in real time enables TSPs to offer payment services that benefit both consumers and merchants. Data aggregators use APIs to connect a mobile wallet app or a merchant's online (or mobile) checkout page with a consumer's bank account: within the app (or the checkout page), a consumer directly logs in to their bank account and the consumer's bank authenticates the account ownership. Data aggregators also facilitate automated clearinghouse (ACH) payments made from a consumer's bank account through real-time verification of sufficient funds in their account.[3] These connections and real-time account balance verification enable mobile wallet providers (such as Venmo) and merchant processors (such as Square) to offer their customers payment services. Mobile wallet providers allow their customers to connect several bank accounts to transfer funds in and out of the mobile wallet and make ACH

payments from their bank accounts. Merchant processors enable their merchants to receive ACH payments for online or mobile transactions. These services benefit merchants because ACH payments are less expensive to accept than credit and debit card payments, and the merchants' risk of not receiving ACH payments due to insufficient funds in the consumer's bank account is significantly reduced. These services also benefit consumers, as they offer more choices of payment methods without sharing the consumers' bank account information with merchants.

In addition to directly enhancing financial services, data aggregators can also increase competition both among financial service providers and across payment methods, thereby improving financial services for both consumers and merchants. Although loan and payment services have been predominantly offered by financial institutions, data aggregators have enabled fintechs and nonbank service providers to offer these services as well. Competition between the new entrants and financial institutions likely results in improved services or lower fees for consumers. Payment services offered by fintechs and nonbank service providers also facilitate competition across payment methods, especially between card payments and bank account-based payments (such as ACH and instant payments), likely reducing costs for merchants to accept payments and increasing payment options for consumers.

Risks associated with data aggregators

Despite the improvements they offer, data aggregators also pose risks for the financial services industry along three dimensions: competition, security, and privacy. The first risk is the potential lack of competition among data aggregators. Because data aggregators' large scale and scope in accessing consumer financial data are beneficial for many parties, the market may allow for only a few large data aggregators.[4] This market structure could lead data aggregators to gain and exercise market power by charging higher fees to TSPs and smaller consumer financial institutions. Therefore, regulators may need to closely monitor the level of competition among data aggregators.[5]

Data security breaches at data aggregators are another risk. In theory, open banking should reduce the number of data breaches that expose consumers' financial account credentials, as those credentials are shared with fewer parties overall. However, open banking is not free from data security breaches. Given the large scale and scope of data aggregators, a data breach at a data aggregator could pose significant risks to financial institutions, including reputational risk and financial losses due to account-takeover fraud. Currently, financial institutions that exchange data with data aggregators are responsible for managing associated risks. As open banking becomes more prevalent and data aggregators store more consumers' financial account credentials, a more robust supervisory framework concerning data aggregators may be needed.[6]

Data aggregators may also pose risks to consumer data privacy. Because APIs offer consumers the ability to control the amount and type of data they share and allow consumers' financial institutions to act as gatekeepers, open banking can improve data privacy relative to screen scraping. Nevertheless, as data aggregators access various consumer data on behalf of TSPs, they may have opportunities to monetize those data. In addition, consumer disclosures may not be adequate or clear enough for consumers to understand who may access their data beyond their authorized TSPs or what they should do to revoke

authorizations given to TSPs to access, use, or store data.[7] For example, simply deleting fintech apps from a mobile phone does not necessarily revoke a consumer's authorizations, and their data may continue to be accessed without their knowledge. Responding to these concerns, regulators have begun to enact policies to protect consumer data privacy. At the federal level, the Consumer Financial Protection Bureau (CFPB) issued Consumer Protection Principles on data sharing and aggregation in 2017. Consumer data privacy will be included in the regulation the CFPB is developing to implement Section 1033 of the Dodd-Frank Act, which provides consumers rights to access their own financial records. At the state level, California, Colorado, Connecticut, Utah, and Virginia have enacted comprehensive consumer data privacy laws. Common provisions of these laws include consumers' right to access and delete personal information and opt out of the sale of personal information, among others (National Conference of State Legislatures 2022).

Conclusion

Data aggregators play a critical role in open banking, enhancing consumer financial services and increasing competition among financial service providers and across payment methods. However, they pose some risks related to data security, data privacy, and low competition among data aggregators. Although regulatory actions are underway in data privacy, regulators may need to monitor the market closely regarding data security and competition.

Endnotes

[1] For simplicity, this example assumes that the consumer's bank has a bilateral data-sharing agreement with the data aggregator.
[2] Generally, to access consumer financial data at a small bank, one API connection is established between a data aggregator and the bank's core banking service provider, and another API connection is established between the core banking service provider and the bank.
[3] In addition to ACH, instant payments may become an open banking-powered payment method soon. Indeed, some open banking apps in the United Kingdom and European Union have started using instant payments (Agarwal and others 2019).
[4] Consolidation has occurred in other markets, such as ATM and debit card markets and ACH operator markets, where a large scale and scope are key market characteristics (Hayashi and others 2003; Rosenbaum and others 2017).
[5] The Department of Justice filed a civil antitrust lawsuit to stop the planned merger between Visa and Plaid in November 2020 and three months later the two companies abandoned their plan (Department of Justice 2021).
[6] Currently, data aggregators are not directly supervised by any federal agency. Although the Consumer Financial Protection Bureau (CFPB) has the authority to supervise nonbank entities such as data aggregators, they are generally not subject to regular federal examination and supervision. The CFPB has authority under the Dodd-Frank Act to designate companies under its supervisory authority as "larger participants" of markets for other consumer financial products or services.
[7] A class action lawsuit against Plaid alleged that the company acted improperly when it obtained users' financial account credentials, which reached a settlement (Geron 2021).

References

Agarwal, Sulabh, Hakan Eroglu, Britta Kotthaus-Krahmer, Amit Mallick, and Tim Grünhage. 2019. "Open Banking + Real-Time Payments: A Match Made in Heaven for Europe." Accenture.

CFPB (Consumer Financial Protection Bureau). 2020. "Consumer Financial Protection Bureau Releases Advance Notice of Proposed Rulemaking on Consumer Access to Financial Records." October 22.

———. 2017. "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation." October 18.

Department of Justice. 2021. "Visa and Plaid Abandon Merger After Antitrust Division's Suit to Block." Press release, January 12.

Geron, Tomio. 2021. "Plaid's Paying $58 Million to End a 98 million-person Privacy Lawsuit." Protocol, August 6.

Hayashi, Fumiko, Richard Sullivan, and Stuart E. Weiner. 2003. "A Guide to the ATM and Debit Card Industry." Payments System Research Department, Federal Reserve Bank of Kansas City: Kansas City, Missouri.

National Conference of State Legislatures. 2022. "State Laws Related to Digital Privacy." June 7.

Rosenbaum, Aaron, Garth Baughman, Mark Manuszak, Kylie Stewart, Fumiko Hayashi, and Joanna Stavins. 2017. "Faster Payments: Market Structure and Policy Considerations." Federal Reserve Bank of Kansas City, Research Working Paper no. 17-14, November.

Julian Alcazar is a payment specialist at the Federal Reserve Bank of Kansas City. Fumiko Hayashi is a policy and research advisor 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.