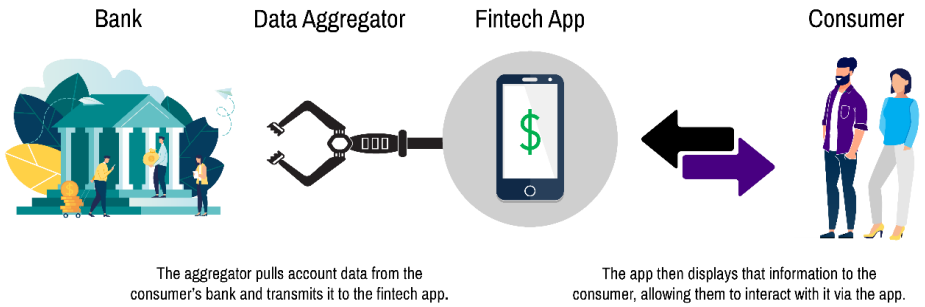
February 20, 2020

Data Aggregators Issue Summary

Banks take seriously their responsibilities to maintain the privacy and security of consumer data and have decades of experience complying with rigorous data security and privacy laws, including the Gramm-Leach-Bliley Act (GLBA). Consumers are increasingly relying on FinTech apps and other nonbank financial services, which are not subject to the same oversight as banks, to help them manage their financial lives.

Data aggregators play a key role in supporting FinTech apps by serving as the digital bridge between apps and banks, linking and instantly verifying financial accounts. For example, Venmo uses a data aggregator to link up with customer bank accounts to facilitate the transfer of the funds. Data aggregators also facilitate personal financial management applications, such as Mint or Personal Capital, allowing consumers to manage financial accounts from different organizations and budget more efficiently. The primary data aggregators within the financial service industry include Plaid; Envestnet's Yodlee; Finicity; MX; Morningstar's ByAllAccounts; Fiserv / CashEdge; Intuit / Mint.



Data aggregators enable FinTech apps to access, aggregate, share and store information from banks and compile consumer financial account and transaction data through (1) screen-scraping or (2) the use of an application programming interface (API).

1. **Screen-scraping:** Consumers input their username and password into the FinTech app, and the data aggregator uses these credentials to access the consumer's accounts. Some apps make it appear as though the bank is directly involved in the login process by using the bank's colors and logos.

2. **API:** APIs are agreed-upon interfaces that link two or more systems, allowing secure authentication and transfer of data. In contrast to screen-scraping, data aggregation through an API generally means that banks are knowingly participating in the sharing of data.

Risks and Concerns Associated with Data Aggregators

The methods by which data aggregators collect and store consumer data put consumers at risk. These data aggregators work in the background, often unbeknownst to consumers. As a result, consumers may be unaware that they are (1) providing their credentials to a third-party data aggregator, rather than directly to a bank; (2) their credentials or data could be further shared and/or used beyond their initial authorized access; and (3) through screen-scraping, data aggregators can gain access to data attributes beyond those needed to provide the product or service requested by the customer.

Given the proliferation of FinTechs and their resulting use of data aggregators to provide quick and easy access to multiple data sources, aggregators have been able to accumulate massive amounts of consumer financial data, with limited standards for safeguarding that data. Without appropriate safeguards or oversight, data aggregators can pose potential risks to consumers related to unauthorized data access and potentially fraudulent activity.

Industry Efforts to Address Risks

The financial services industry, including banks, some FinTechs and certain data aggregators, has taken steps to improve financial data sharing while protecting consumer data and privacy. These initiatives are necessary steps to mitigate the above risks associated with the use of data aggregators.

- **Financial Data Exchange (FDX) – Common API**: FDX, a nonprofit consortium of banks, FinTechs, data aggregators and consumer groups, developed a common API to standardize security and authentication around data transfer, intended to improve security for the customer and create predictability for the industry. FDX is also developing user experience and consent guidelines to promote responsible data sharing across participants.
- **The Clearing House – Connected Banking Initiative:** The Clearing House (TCH) is leading a Connected Banking initiative to create a system that inspires trust and enables sustained innovation. As a part of this effort, TCH developed a Model Agreement that banks, data aggregators and FinTechs can use as a reference to facilitate and expedite bilateral data-sharing agreements. TCH is also piloting a streamlined risk assessment process for third-party due diligence.
- **Akoya – Data Access Network**: Akoya's Data Access Network facilitates direct connections utilizing FDX's API by providing a single point of integration for data providers and data recipients. Akoya's one-to-many API connections reduces the need for creating specific bilateral data access agreements by providing single contract and approval process for connection between banks, aggregators and FinTechs.
- **Consumer Financial Protection Bureau (CFPB) – Principles for Consumer-Authorized Financial Data Sharing and Aggregation:** The CFPB published principles for protecting consumers when they authorize third-party companies to access their financial data to provide certain financial products and services.[1] These principles have served as a guide for banks' approach to data aggregators and helped facilitate industry efforts described above. The CFPB signaled further interest in advancing consumer access to financial records through the issuance of an Advance Notice of Proposed Rulemaking, on which BPI provided comments.[2]

BPI's Position

Data Aggregators Should Be Held to the Same Rigorous Data Security and Privacy Standards as Banks
Banks have legal obligations to safeguard customer data and comply with strict regulatory requirements related to privacy and security, and have put decades of effort into protecting their customers and institutions. In comparison, aggregators' security controls vary, some may lack the capability to comply with disclosures required under privacy laws and they are not subject to supervision by regulators similar to that of banks. At a minimum, the CFPB and other agencies should clarify that data aggregators should have in place similar standards as those provided under Regulation P[3] and the Interagency Guidelines Establishing Information Security Standards[4], the implementing regulations of GLBA, for the purposes of consumer data security and privacy.

Data Aggregators Should Be Transparent in How They Access and Use Consumer Data
Consumers should have a better understanding of the risks associated with sharing their financial data. To that end, data aggregators should be required to obtain affirmative consent to access consumers' financial data that is narrowly tailored to and commensurate with how the data will be accessed, obtained and used. Additionally, consumers should have the ability to confirm, modify and revoke access once granted, and a clear and easy process to do so.

Liability for Unauthorized Transactions and Cyber Breaches Must Be Addressed
BPI believes there is a lack of clarity around the level of responsibilities aggregators share in the event of unauthorized transactions and cyber breaches and supports clarification of liability during such occurrences. Banks should practice due diligence on data aggregators and manage connectivity risk but should not be held liable for a loss of customer data due to the activities of a data aggregator.

Industry Should Adopt APIs for Data Sharing
BPI applauds industry efforts such as FDX's common API, but more must be done to move away from the practice of screen-scraping. BPI encourages banks, data aggregators and interested stakeholders to work together to enable migration towards API-based data sharing. Data sharing should consider the adoption of secure token standards and provide customers visibility and control into personal data shared between FinTech apps and banks.

---

[1] *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation,* Consumer Financial Protection Bureau, October 2017, https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf
[2] See BPI's comment letter response to the CFPB's ANPR on Section 1033 of the Dodd-Frank Act here: https://bpi.com/wp-content/uploads/2021/02/BPI-Comment-Letter-Responding-to-CFPB-1033-ANPR-2021.02.04.pdf.
[3] 12 C.F.R Part 1016
[4] 12 C.F.R. Appendix B to Part 30