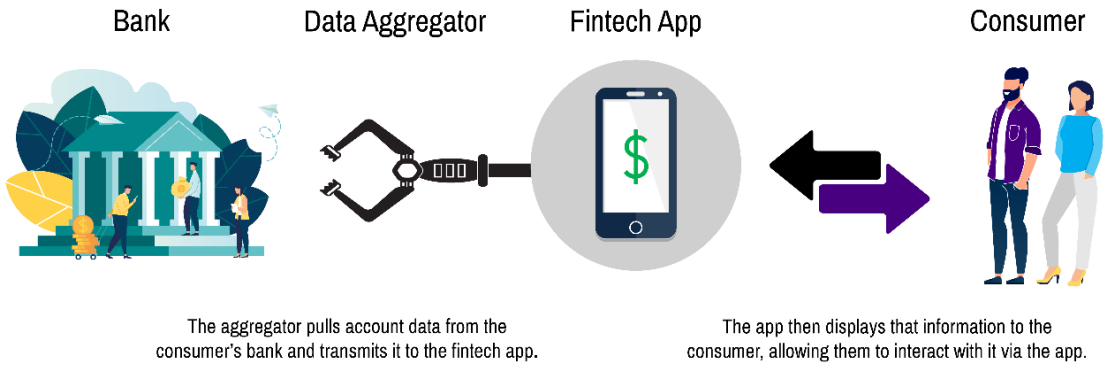
Data Aggregators Issue Summary

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).[1] 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.



Data aggregators connect FinTech apps to 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

Data aggregators provide an important function in facilitating the delivery of personalized and convenient financial services. However, the methods by which data aggregators collect and store consumer data puts consumers at risk.

- **Consumers Lack Clarity on Data Provided to Third Parties:** 80 percent of FinTech users are not aware that apps may access their bank account username and password.[2] When consumers provide their account login credentials to a FinTech app, they may not realize that they are providing their credentials to a third-party aggregator who will often access information through screen-scraping and not by logging directly into their financial institution.
- **Aggregators Access and Store Data without Approval:** After providing credentials and other information, aggregators store this information indefinitely to enable constant updating of account information. Aggregators can theoretically reuse, repurpose or sell a consumer's credentials without further approval. The Financial Industry Regulatory Authority (FINRA) issued a dire warning to consumers about the dangers of sharing account data with aggregators and highlighted the heightened security risks with aggregators storing consumer financial information and credentials.
- **Aggregators Increase the Potential for Fraudulent Activity:** Consumers are increasingly being exposed to unauthorized transactions and potentially fraudulent activity related to the use of data aggregators. FinCEN Director Kenneth Blanco warned that cybercriminals appear to be using data aggregators to facilitate account takeovers and create fraudulent accounts as part of identity theft or synthetic identity fraud.[3]

[1] See Financial Trades Letter to NTIA on "*Developing the Administration's Approach to Consumer Privacy,*" November 8, 2018. Available at https://bpi.com/wp-content/uploads/2018/11/Financial_Trades_-NTIA_Comment_LetterNov.8.2019.pdf
[2] *Consumer Survey: Financial Apps and Data Privacy,* The Clearing House, November 2019
[3] Brendan Pederson, "Bad Actors Targeting FinTech Aggregators: FinCEN Chief," *American Banker,* 24 September 2019

- **Questionable Liability During a Cyber Breach:** Banks are concerned about the potential for a cyber breach of data aggregators considering aggregators collect and store significant amounts of customer account data. 70 percent of consumers believe that the financial app should be responsible during a data breach;[4] however, there is a lack of clarity around the level of responsibilities aggregators share should a breach occur. If an aggregator is breached, banks worry that they will be held liable for the stolen data even if they are not at fault.

Industry Efforts to Address Risks

The financial services industry, including banks, 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 APIs**: FDX, a nonprofit subsidiary of the Financial Services Information Sharing and Analysis Center (FS-ISAC), 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.
- **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.
- **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.[5] 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 Advanced Notice of Proposed Rulemaking, on which BPI provided comments.

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[6] and the Interagency Guidelines Establishing Information Security Standards[7], 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

Screen-scraping allows an aggregator to obtain significantly more data than needed by the underlying FinTech app, including sensitive personal information, which could subsequently be stolen. Consumers should have a better understanding of the risks associated with sharing their financial data. To that end, 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.

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 efforts by FDX to create a common API and by TCH to promote safe methods of sharing customer financial data, 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.

---

[4] *Consumer Survey: Financial Apps and Data Privacy,* The Clearing House, November 2019

[5] *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

[6] 12 C.F.R Part 1016

[7] 12 C.F.R. Appendix B to Part 30