BANK POLICY INSTITUTE

Statement by the Bank Policy Institute

Before the U.S. House Committee on Financial Services Task Force on Financial Technology
"Preserving the Right of Consumers to Access Personal Financial Data"

September 21, 2021

Chair Waters, Ranking Member McHenry, Task Force Chair Lynch, Ranking Member Davidson and Members of the Fintech Task Force:

We support the ability of bank customers to securely connect their bank accounts to the third-party apps of their choice, which, in some cases, may involve the interposition of a data aggregator to collect the customer's information from the customer's financial institution and provide it to the app. It is critical, however, that consumers' personal and financial information remains secure when it is shared between financial institutions and third parties. Ensuring the security of customer data is, and will remain, a top priority for the banking industry. Consumer-permissioned financial data sharing should be guided by the following three principles:

- First, consumer financial information should be *safe and secure* regardless of who holds it;
- Second, *informed consumer consent* should be a precondition to any sharing of consumer financial information; and
- Third, the consumer should have *effective control* over the type and amount of information that is shared.

In light of these principles, we strongly support the migration of connections between financial institutions and data aggregators to secure Application Programming Interfaces, or APIs, that can support informed customer consent and control over their information and the secure transmission of this properly permissioned information.

We also support robust federal supervision and examination of entities like data aggregators and third-party data users that hold consumers' sensitive financial data.

Lastly, as it is the consumers' financial health and security that is at risk when their data is shared, the Consumer Financial Protection Bureau (CFPB) and other federal regulators should empower consumers to effectively control the sharing and use of their financial data. To do that, consumers need sufficient information and clear mechanisms of control in order to make informed decisions about: (i) the parties they are sharing their data with, (ii) the duration and frequency of permissioned access they are granting, (iii) the specific data elements they are sharing, (iv) the ability to revoke the access, (v) the ability to require third and fourth parties to delete their data, and (vi) the purposes for which third parties may use their data.

THE CURRENT STATE OF DATA AGGREGATION: OBSCURE AND INSECURE

Data aggregators play a key role in enabling fintech apps to access, aggregate, share and store information from banks and compile consumer financial account and transaction data. However, data aggregators work in the background, often unbeknownst to consumers, and the methods by which data aggregators collect and store consumer data puts consumers at risk.

After a consumer shares his or her credentials to facilitate access to a fintech app, aggregators are able to collect and store those credentials, and gain access to consumer data attributes through screen scraping activities. It is difficult to estimate the quantity of data held by data aggregators, of which there are approximately 120 in the United States. According to one report, data aggregator Acxiom provided up to 3,000 attributes on 700 million

people in 2017, and by 2018, it had collected 10,000 attributes on 2.5 billion consumers.[1] While these figures are difficult to verify, we can be certain that the largest data aggregators hold the sensitive financial information of millions of U.S. consumers.[2]

Unfortunately, many consumers lack an understanding of how their financial information is being collected, shared, and stored. A November 2019 survey conducted by The Clearing House (TCH), a banking association and payments company, found that more than 80% of financial app users are not aware that apps may use third parties to access consumers' personal and financial information, and 80% of financial app users are not fully aware that apps or third parties may store their bank account username and password.[3]

RISKS OF SCREEN SCRAPING AND CREDENTIAL-BASED ACCESS

The use of screen scraping and credential-based access is both outdated and unsafe. First, this method does not allow consumers to control the amount of data they share with third parties, and there is no way to ensure that the information "scraped" and maintained by the aggregator does not go beyond what is necessary for the financial app to deliver the services sought by the consumer. Additionally, there is the risk that the aggregator or third-party app may continue to collect and store the consumer's data and credentials even after the consumer ceases using the financial app.

Second, screen scraping, and the credential-based access on which it is based, creates opportunities for malicious actors to gain access to a consumer's accounts at a financial institution and commit fraud, or even take over the consumer's account. As former FinCEN Director Kenneth A. Blanco has previously warned: "In some cases, cybercriminals appear to be using fintech data aggregators and integrators to facilitate account takeovers and fraudulent wires. By using stolen data to create fraudulent accounts on fintech platforms, cybercriminals are able to exploit the platforms' integration with various financial services to initiate seemingly legitimate financial activity while creating a degree of separation from traditional fraud detection efforts."[4]

Third, screen scraping can divert the cybersecurity resources of regulated financial institutions away from preventing truly unauthorized access by criminals or other bad actors, because in many cases, it is difficult for a financial institution to distinguish "legitimate" data aggregator logins from illegitimate traffic. This problem is compounded by the fact that some data aggregators bypass security controls used by financial institutions to authenticate customer logins (such as by auto-populating the security questions posed when a new connection is sought to be established with a consumer's account). As the Basel Committee on Banking Supervision found in its 2019 "Report on open banking and application programming interfaces": "Screen scraping or reverse engineering can undermine a bank's ability to identify fraudulent transactions, as banks cannot always distinguish between the customer, data aggregator, and an unauthorised third party that is logging in and extracting sensitive data."[5]

MIGRATION TO APIS FOR CONSUMER FINANCIAL DATA SHARING

The use of APIs for consumer permissioned financial data sharing is widely considered to be more safe and secure than screen scraping, as APIs allow data to be shared without the use of consumer credentials and provide enhanced control over the type and extent of data shared. Several industry efforts have advanced the adoption of APIs in the United States. For example, the Financial Data Exchange developed a common API technical standard for data sharing through an industry consortium of banks, data aggregators, fintechs and consumer groups. Over

[1] https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information.
[2] Natalie S. Talpas, PNC Bank, Consumer Financial Protection Bureau Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act, Feb. 26, 2020, available at: https://files.consumerfinance.gov/f/documents/cfpb_talpas-statement_symposium-consumer-access-financial-records.pdf
[3] The Clearing House, Consumer Survey: Financial Apps and Data Privacy, November 2019, available at: 2019-tch-consumersurveyreport.pdf (theclearinghouse.org).
[4] Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered at the Federal Identity (FedID) Forum and Exposition, *"Identity Attack Surface and a Key to Countering Illicit Finance"*, (September 24, 2019), *available at* https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-federal-identity-fedid
[5] Basel Committee on Banking Supervision, "Report on open banking and application programming interfaces" (November 2019), *available at*: Report on open banking and application programming interfaces (APIs) (bis.org).

22 million consumers are now using FDX's API for data sharing in North America.[6] Additionally, banks and data aggregators have entered into data access agreements to facilitate the dating sharing process through APIs and to specify how data is accessed and protected.

Despite the industry's progress, screen scraping remains a widely used method for accessing payments account data, enabling data harvesting of credentials to continue. Government action to outlaw screen scraping, either through an act of Congress or coordination between the CFPB and the federal banking agencies in implementing section 1033 of the Dodd-Frank Act, which provides the CFPB with authority to promulgate rules around consumer financial data sharing, would accelerate the migration of consumer data sharing to APIs. The technology exists today to migrate to APIs, but market participants may not have the incentive to transition to APIs if screen scraping is allowed to continue. The migration of thousands of banks, data aggregators and fintechs in the United States to APIs for sharing consumer data would be a significant undertaking, particularly for those banks that may not have actively participated in the market-driven movement towards APIs that has occurred to date. Indeed, this process could take several years to complete. For this reason, it is critical to establish a specific timeline *now* to end screen scraping so that all market participants begin to work towards a future ecosystem wherein all consumers are able to share their information on an informed basis in a safe and secure manner.

DATA AGGREGATORS SHOULD BE SUBJECT TO SYSTEMATIC CYBERSECURITY OVERSIGHT

Under the current framework, data aggregators access and store similar information to that of banks, but are not held to similar standards for safeguarding consumer data. The CFPB has the authority under the Dodd-Frank Act to define the universe of larger nonbank participants in the data aggregator market. The CFPB should initiate a rulemaking under this authority, which would then give the Bureau the authority to supervise and examine those entities for compliance with applicable data security standards and consumer financial laws, just as banks are regularly examined for compliance with the GLBA's information security standards and consumer financial protection laws. Further, the CFPB should apply these GLBA standards to data aggregators and other authorized entities. The FFIEC examination guidance on information security also could serve as a useful model for the Bureau in developing the appropriate information security standards for large nonbank data aggregators and data users.[7]

CONSUMER TRANSPARENCY AND CONTROL

Simply put, consumers should have full awareness and control over how their data is shared and used. To that end, consumers should be made aware that a data aggregator or other third party is being interposed between the customer's bank and a third-party app and of the accounts and data fields that will be accessed by data aggregators and data users. Consumers cannot make informed choices without transparent and readily accessible disclosures. As the CFPB stated in its principles for consumer-authorized financial data sharing, firms seeking to obtain consumer authorization for sharing their financial data should provide clear disclosures regarding the "identity and security of [the] party, the data they access, their use of such data, and the frequency at which they access the data … throughout the period that the data are accessed, used, or stored."[8]

Consumers must have the ability to consent to share their financial data, and the ability to confirm, modify and revoke access once granted. As a minimum safeguard, data aggregators and data users should be required to periodically require consumer re-authorization to access consumer data. Perpetual access permissions unnecessarily put consumers and their data at risk. Ideally, data aggregators and data users should be required to obtain the consumer's additional affirmative consent before they are allowed to use the consumer's data for a secondary use not reasonably expected by consumers, thereby empowering consumers to control all the potential uses by permissioned parties of their data.

Similarly, consumers should also have control over the duration of their consent to a third party's accessing their

[6] *See* Financial Data Exchange (FDX) Reports 22 million Consumer Accounts on FDX API.
[7] FFIEC, Information Technology Examination Handbook, Information Security Booklet, *available at* https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
[8] Consumer Financial Protection Bureau, "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation" (Oct. 18, 2017), Principle 6, *available at* https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

data. Currently, many consumers are not aware that deleting an app from their phone does not revoke the app's ability (or that of the app's data aggregator, if any) to continue to access the consumer's financial data. Indeed, Federal Reserve Board Governor Lael Brainard has observed, "[w]hen a consumer deletes a fintech app from his or her phone, it is not clear this would guarantee that a data aggregator would delete the consumer's bank login and password, nor discontinue accessing transaction information."[9]

In addition, data minimization is a fundamental security principle: limiting the dissemination of sensitive data reduces the consumer's risk of exposure. Unfortunately, the natural incentives of data aggregators and data users may not necessarily be aligned with this principle. Consumers therefore should be able to limit what data a third party can access and the purposes for which the data may be used.[10]

The right to data deletion also is an important and effective way consumers can protect themselves from future data breaches. And while the CFPB's second principle states that "[t]hird parties with authorized access … [should] only maintain such data as long as necessary," many data aggregators and data users do not make it easy for consumers to exercise this right, to the extent they provide this right at all.[11] Federal Reserve Board Governor Lael Brainard recognized this problem, noting that "[i]f a consumer severs the data access, for instance by changing banks or bank account passwords, it is also not clear how he or she can instruct the data aggregator to delete the information that has already been collected. Given that data aggregators often don't have consumer interfaces, consumers may be left to find an email address for the data aggregator, send in a deletion request, and hope for the best."[12]

CONCLUSION

BPI supports consumers' ability to access and share their personal financial data. It is of paramount importance that this data is shared based on informed consumer consent and effective consumer control over the type and amount of information that is shared and that the data is maintained in a safe and secure manner regardless of where, why or with whom that data is maintained.

[9] Lael Brainard, "Where Do Consumers Fit in the Fintech Stack?" (Nov. 16, 2017), *available at* https://www.federalreserve.gov/newsevents/speech/brainard20171116a.htm.

[10] Consumer Financial Protection Bureau, "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation" (Oct. 18, 2017), *available at* https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf. Principle 2 states that participants should "only access the data necessary to provide the product(s) or service(s) selected by the consumer."

[11] *Id.*

[12] *See* note 8, *supra*.