BANK POLICY INSTITUTE

October 3, 2022

Via electronic submission

Hon. Rohit Chopra
Director
Consumer Financial Protection Bureau
1700 G Street, NW Washington, D.C. 20552

Re: Joint trades petition for rulemaking defining larger participants of the aggregation services market

Dear Director Chopra:

We write regarding the petition submitted by the American Bankers Association and several other trade organizations to the CFPB pursuant to Section 553(e) of the Administrative Procedure Act to engage in a rulemaking to define larger participants in the market for aggregation services.[1] The joint trades' petition requests that the CFPB "define larger participants of a market for aggregation services" and "to the extent necessary . . . to define the term "aggregation service" as a "financial product or service" for purposes of title X of the Dodd-Frank Act."

As discussed further herein, the Bank Policy Institute supports this petition, as a larger participant rulemaking for data aggregation services would help ensure that consumers' sensitive data is subject to consistent and robust protections akin to those provided by banks regardless of what entity holds that data while allowing innovation in the financial services marketplace to continue apace.[2]

I. Background

In the United States, shifts in consumer demand for more digital and interactive financial products and services have dramatically changed the marketplace, which now includes an increasing number of fintechs and other technology companies not subject to the same comprehensive regulatory

[1] Petition to The Consumer Financial Protection Bureau for rulemaking defining larger participants of the aggregation services market, American Bankers Association, Consumer Bankers Association, Credit Union National Association, Housing Policy Council, Independent Community Bankers of America, National Association of Federally-Insured Credit Unions, National Bankers Association, and The Clearing House Association (August 2, 2022), available at: Regulations.gov.

[2] The Bank Policy Institute is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost two million Americans, make nearly half of the nation's small business loans, and are an engine for financial innovation and economic growth.

oversight as banks, but increasingly facilitating access to sensitive consumer data to provide such products and services.

This surge in adoption of digital products and services has accelerated banks' efforts to leverage market-developed technological solutions to help meet customer demand while ensuring consumers' sensitive financial data is kept private and secure. Unlike other jurisdictions in which consumer financial data sharing has been mandated by government action, this expansion of consumer data access in the United States has developed via innovation in the marketplace. Under an industry-driven approach, participants can innovate and adapt more quickly to market changes and develop safer solutions through agreements that benefit both the market and consumers.

BPI supports innovation and welcomes competition in payments and other financial products and services when this innovation is conducted responsibly and in a way that ensures consumers are protected through consistent regulation and oversight. In this regard, BPI supports the ability of bank customers to securely connect their bank accounts to the third-party apps of their choice. In some cases, this connection may involve the interposition of a data aggregator to collect the customer's information from a 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 consumer data is, and will remain, a top priority for the banking industry.

Banks use a variety of measures and technologies to identify and defend against fraud, and banks are required by law and regulation to protect consumer data and establish and maintain robust programs for this purpose. Further, banks are regularly examined for compliance with these requirements, while nonbanks, including data aggregators and other entities operating in the data aggregator market, largely are not. Unless all entities in the ecosystem are subject to the same legal requirements and oversight for security and fraud detection, consumer fraud could expand dramatically while the ability to combat it could diminish.

Pursuant to Section 1024 of the Dodd-Frank Act, the CFPB has authority over "any covered person who… is a larger participant of a market for other consumer financial products or services, as defined by rule."[3] To date, the CFPB has defined "larger participants" in the consumer reporting, consumer debt collection, student loan servicing, international money transfer, and automobile financing markets, which has allowed the agency to examine the activities of these larger participants in a similar manner to those covered persons routinely supervised by the CFPB pursuant to Section 1025.[4]

BPI supports consistent and robust federal supervision and examination of entities like data aggregators and third-party data users that retrieve data from data holders -- banks, credit unions, and providers of core transaction accounts -- and supports the petition to the CFPB to initiate a rulemaking to define larger market participants in the data aggregation market. This action alone will help further

[3] 12 U.S.C. §5514 (a)(1)(B). A "covered person" is "(A) any person that engages in offering or providing a consumer financial product or service; and (B) any affiliate of a person . . . if such affiliate acts as a service provider to such person." 12 U.S.C. 5481(6).

[4] 12 C.F.R. 1090.

multiple CFPB strategic goals.[5] Indeed, BPI has made this recommendation in the past.[6]

II. The market for data aggregation services.

The CFPB has observed that "[i]n authorizing a third party to access consumer data, consumers engage in a broad and complex ecosystem that enables such access", the main participants in which are consumers; data holders; data users; and data aggregators.[7] These are the primary participants in the market for data aggregation services.

Data holders are covered persons "with control or possession of consumer financial data" and include providers of consumer financial products and services that, in the ordinary course of their business, collect, generate, or otherwise possess and retain information about consumers' use of their products and services.[8] Data holders are generally understood to be banks, credit unions, and other providers of core transaction accounts.[9]

The CFPB has described data users as "a third party that uses consumer-authorized data access to provide either (1) products or services to the authorizing consumer or (2) services used by entities that provide products or services to the authorizing consumer."[10]

Data aggregators typically access and transmit consumer financial data to data users pursuant to consumer authorization. Indeed, the CFPB has characterized data aggregators as "fourth parties" that "support data users and/or data holders in enabling authorized data access."[11] In other words, data aggregators interpose themselves between data holders (banks) and data users (apps) to enable consumers to authorize the transfer of their information to the app of their choice. The CFPB has noted, however, that the three categories of "data holder, data user, and data aggregator" "are not mutually exclusive in theory or in practice."[12]

Consumer-permissioned access to authorized data has increased competition in the provision of financial services to consumers. Banks are highly incentivized to facilitate consumer-authorized data

---

[5] *See* CFPB Strategic Plan FY 2022 to FY 2026, p.9.

[6] *See* BPI comment letter re: Advance Notice of Proposed Rulemaking issued by the Consumer Financial Protection Bureau seeking input on consumers access to financial records pursuant to Section 1033 of the Dodd-Frank Act. 85 Fed. Reg. 71003 (Nov. 6, 2020); available at: BPI-Comment-Letter-Responding-to-CFPB-1033-ANPR-2021.02.04.pdf; *see also* BPI Statement Before House Task Force on Financial Technology on Consumer Access to Personal Financial Data (September 21, 2021), available at: BPI Statement Before House Task Force on Financial Technology on Consumer Access to Personal Financial Data - Bank Policy Institute.

[7] CFPB: Advance Notice of Proposed Rulemaking on Consumer Access to Financial Records (November 6, 2020) 85 FR 71003, 71005 (Nov. 6, 2020), available at: 2020-23723.pdf (govinfo.gov).

[8] 85 FR 71004.

[9] 85 FR 71005.

[10] 85 FR 71004.

[11] *Id*.

[12] 85 FR 71006.

access as a means of increasing consumer satisfaction and enhancing consumers' digital experience. The banking industry has been working for years to develop technical solutions that enable consumer-permissioned access to financial data while providing data protections, including through collaborations between banks, fintechs, and data aggregators that demonstrate how the industry has progressed the data sharing marketplace to better serve and protect consumers.

First, the industry continues to move away from screen scraping and credential-based data access towards data sharing through Application Program Interfaces (APIs), which facilitate the transfer of consumer financial data through tokenized access, thus removing credential sharing and allowing users to be securely authenticated at their own financial institution.[13] Credential sharing generally enables a data aggregator to access – and "scrape" – all of a consumer's financial information, even if the consumer has provided the aggregator or user limited authorization to access information from a data holder. Access to excess data beyond the scope of the consumer's intended authorization increases the potential for consumer harm. Data sharing through APIs using tokenization is more accurate and secure than screen scraping and credential-based data access, and continued adoption of APIs and increased use of tokenization will benefit consumers and all market participants.[14]

Importantly, the financial services industry collectively has advanced the marketplace towards common technical standards for the secure access of consumer-permissioned data. Several industry efforts have developed API's and promoted their adoption in the United States. For example, FDX developed a common API technical standard for data sharing through an industry consortium of banks, data aggregators, fintechs and consumer groups. As of June of this year, 32 million consumers were using FDX's API for data sharing in the United States and Canada.[15]

Additionally, banks and data aggregators have entered into data access agreements to facilitate the data sharing process through APIs. These agreements benefit and protect consumers as they specify how data is protected and how and when data is accessed. The industry also is moving towards utilizing networks to facilitate access and broader adoption. For example, Akoya's Data Access Network facilitates direct connections utilizing FDX's API by providing a single point of integration for data providers and recipients and reducing the need for creating specific bilateral data access agreements.[16]

---

[13] The CFPB has stated that "'Credential-based access'' refers to authorized access that uses the consumer's user ID and password or like credentials to log into the data holder's online financial account management portal, generally on an automated basis. 'Screen scraping' refers to authorized access that uses proprietary software to convert consumer data presented in the provider's online financial account management portal into standardized machine readable data, again generally on an automated basis. Credential-based access and screen scraping often are described collectively as 'screen scraping.' But while the two practices typically are linked, they are technically and conceptually distinct." 85 FR 71006 at note 15.

[14] U.S. Department of Treasury, *A Financial System That Creates Economic Opportunities – Nonbank Financials, Fintech and Innovation* (July 2018), available at: https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation.pdf.

[15] *See* Press Release, "Financial Data Exchange (FDX) Reports 32 Million Consumer Accounts Use FDX API for Open Finance and Open Banking" (June 27, 2022), available at: Financial Data Exchange (FDX) Reports 32 Million Consumer Accounts Use FDX API to Power Open Banking.

[16] *See*, e.g., Press Release, "U.S. Bank and Akoya team up to accelerate safe, secure, and transparent consumer-permissioned financial data access", available at: Akoya and U.S. Bank team up to accelerate safe, secure, and

Akoya connects multiple fintechs and data aggregators with data providers, which can reduce costs for financial institutions, including community banks, by eliminating the costs associated with developing and maintaining APIs on their own and with negotiating multiple data access agreements.

However, despite the industry's progress, screen scraping remains a widely used method for accessing payment account data, enabling the collection, retention and use of consumers' bank account credentials to continue and increasing risks of data breaches of consumers' sensitive personal and financial data, which may result in fraud and other consumer harm.

While data aggregators access consumers' financial account transaction data with proper authorization and share it with a data user to fulfill a specific consumer-authorized purpose, data aggregators may also use this permissioned access to harvest more data than is necessary and/or retain the data collected, even after it has been shared with the data user on whose behalf it was collected. If aggregators retain consumers' credentials and the aggregator is hacked, there is a risk that bad actors may then use consumers' credentials to access their accounts, exposing consumers to the risk of theft or fraud. In addition, aggregators may sell consumer data to third parties.

All of these concerns are very real given the huge volume of highly sensitive consumer data that data aggregators and users collect and retain. It is difficult to estimate the quantity of data held by data aggregators, of which there are approximately 120 in the United States. As of 2020, one large data aggregator connected to 200 million consumer bank accounts across 11,000 U.S. banks, and likely connects to even more accounts and banks today.[17] While these figures are difficult to verify, it is indisputable that the largest data aggregators, most of which are currently unregulated, hold the sensitive financial information of millions of U.S. consumers. Furthermore, many consumers lack an understanding of how their financial information is being collected, shared, and stored, and for how long it is being stored, and thus would have no reason to monitor the privacy and security practices of data aggregators or data users to demand that robust data protection protocols be adhered to.

Today, the only backstop on unchecked use by aggregators and other downstream parties is bilateral data sharing agreements between data holders and aggregators. Customers should not be at the mercy of their bank's ability to restrict secondary use of their sensitive personal banking information. Instead, a regulatory scheme to comprehensively cover data protection is optimal to encourage wide and safe adoption of consumer permissioned data sharing while ensuring consistent compliance with applicable Federal consumer financial laws. With regulation and oversight harmonized across all parties, market participants can focus more on developing business cases that protect and benefit consumers.

A December 2021 consumer survey conducted by The Clearing House found that 80% of consumer respondents were largely unaware that apps use third-party providers to gather users' financial data; only 24% knew that data aggregators can sell personal data to other parties for marketing, research, and other purposes; 73% were unaware that fintech apps have access to their bank

---

transparent consumer-permissioned financial data access | Company blog | U.S. Bank (usbank.com) (Nov. 16, 2020); *see also* Akoya website at https://www.akoya.com/.

[17] Press Release *"Justice Department Sues to Block Visa's Proposed Acquisition of Plaid"*, (November 5, 2020), available at: https://www.justice.gov/opa/pr/justice-department-sues-block-visas-proposed-acquisition-plaid.

account username and password; and 78% did not know that aggregators regularly access personal data even when the app is closed or deleted.[18]

III. Data aggregators and nonbank data users lack sufficient data security controls and oversight for their data security practices.

Although financial institutions, data aggregators and fintechs store similar data, banks are subject to more stringent expectations and oversight regarding the security controls used to maintain the safety and privacy of that data. Federal banking organizations are subject to numerous laws and regulations that govern how consumer data can be collected, used, and retained and how it must be secured. Indeed, over many years, banks have developed sophisticated systems to protect consumer data and to detect, prevent, and respond to cyber threats. These efforts include multiple levels of internal oversight including by the board of directors, regular participation in cross-industry threat information sharing programs to identify and defend against malicious actors, and robust training and exercise programs to test protective measures. These activities are subject to extensive regulatory oversight and examination to ensure such protections are in place and can include financial penalties or restrictions on activities for failure to comply.

In particular, banks are subject to the Gramm-Leach-Bliley Act and its implementing regulations that require maintaining consumer data privacy, extensive guidelines from the Federal Financial Institutions Examination Council Information Technology handbooks,[19] and the federal banking agencies' third-party risk management guidelines.[20] The federal banking agencies issued the Interagency Guidelines Establishing Information Security Standards pursuant to GLBA, which require banks to develop, implement, and maintain an information security program to identify and control risks to consumer information and systems.[21] The Interagency Guidelines also require banks to perform regular risk assessments and conduct "appropriate due diligence" in selecting and monitoring service

[18] The Clearing House, 2021 Consumer Survey: Data Privacy and Financial App Usage 3 (Dec. 2021), available at: 2021-TCH-ConsumerSurveyReport_Final (theclearinghouse.org).

[19] FFIEC IT handbooks are used in the supervision of financial institutions and cover topics such as information security, management, technology architecture and operations, and retail payment systems.

[20] The federal banking agencies also have issued "Third Party Risk Management Guidelines" that outline the expectations for banks to manage the risks of counterparties with whom they have business relationships. The agencies recently proposed amendments to this guidance and requested comment on the extent to which banking organization may have "business arrangements" and third-party relationships with data aggregators, and therefore should manage these relationships consistent with the third-party risk management guidance." BPI submitted a comment on the proposed amendments to the TPRM Guidance and stated that data aggregators — including both those that engage in unilateral "screen-scraping" and those with which a banking organization may have a contract or other data sharing relationship — can pose meaningful risks to banking organizations and their customers but that the TPRM practices and expectations described in the Proposed Guidance would not be appropriate for either type of activity for several reasons. However, the ultimate expectations of the regulators in this regard remain unclear at this point. *See* BPI's comment letter in response to the "Proposed Interagency Guidance on Third-Party Relationships," available at: BPI Comment Letter - Interagency Guidance on Third Party Relationships (Docket ID(7661407.20).docx.

[21] 12 C.F.R. pt. 30, App. B. *See* 66 Fed. Reg. 8616 (February 1, 2001). These guidelines are currently codified at 12 CFR pt. 30, Appendix B (OCC); Regulation H, 12 CFR 208, Appendix D-2 (Board); Regulation Y, 12 CFR 225, Appendix F (Board); 12 CFR pt. 364, Appendix B (FDIC).

providers.[22] The federal banking agencies also issued the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice which outlines requirements relating to programs for incident response, including customer and regulator notification.[23] To ensure compliance with these requirements and others, banks are regularly examined by prudential regulators.

As a part of implementing the GLBA, the FTC promulgated the Safeguards Rule, which the FTC recently updated, which sets forth specific criteria relating to the safeguards that certain nonbank financial institutions must implement as a part of their information security programs.[24] These safeguards, among other things, limit who can access consumer information, require the use of encryption to secure such information, and require the designation of a single qualified individual to oversee an institution's information security program and report at least annually to the institution's board of directors or equivalent governing body.[25]

The FTC has indicated that data aggregators and consumer fintech application providers significantly engaged in financial services and products are financial institutions under GLBA and are therefore subject to the Safeguards Rule.[26] However, while the data security provisions of the GLBA are enforced by the federal banking agencies for depository institutions, and the SEC and CFTC for entities under their jurisdiction, the FTC does not have the authority to routinely supervise and examine institutions for compliance with GLBA provisions. Further, there is no federal standard for consumer or regulator notification in the event of a data breach by a data aggregator.

Data aggregators' security controls vary, and these firms are not subject to regular supervision to ensure appropriate compliance with applicable Federal laws and supervisory expectations. Without appropriate safeguards or oversight, data aggregators can pose potential risks to consumers related to unauthorized data access. For example, consumers face risks when they part with their banking credentials, which, when stolen, may enable identity theft, theft of funds, and even the ability to take control of the account. Additionally, without requirements for information security programs, the potential for a data breach at a data aggregator may result in misuse of consumer data. Nor are nonbank participants in the data aggregator marketplace subject to regular, direct regulation or supervision for privacy, security, prudential, or consumer protections, in contrast to federally regulated banks, thereby further exacerbating these risks. The CFPB recently issued Consumer Financial Protection Circular 2022-04, which provides that having "insufficient data protection or security for sensitive consumer information" can be a violation of the prohibition on unfair acts or practices in the

[22] 12 C.F.R. pt. 30, App. B, III D.

[23] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736 (March 29, 2005), available at: 05-5980.pdf (govinfo.gov).

[24] 86 Fed. Reg. 70272 (December 9, 2021).

[25] 86 Fed. Reg. 70272 (December 9, 2021).

[26] Federal Trade Commission, Financial Institutions and Customer Information: Complying with the Safeguards Rule (Apr. 2006), available at: https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutionscustomer-information-complying (stating that the Safeguards Rule applies to companies that receive information about the customers of other financial institutions).

Consumer Financial Protection Act.[27] However, again, most data aggregators and data users in the data aggregator marketplace are not subject to regular, direct supervision or examination by the CFPB or any other federal regulator. Absent regular supervision and examination, data protection shortcomings at the largest data aggregators might not be identified until after a breach and significant consumer harm have occurred.

Section 1033 of the Dodd-Frank Act provides the CFPB with authority to promulgate rules regarding consumer access to financial records and data sharing. The CFPB has taken several steps to gather information about the consumer data sharing ecosystem but has not yet issued proposed rules to implement Section 1033.[28] Rulemaking in this regard could help enhance the security of increased data sharing but does not negate the need for the CFPB to initiate a rulemaking process to define larger market participants in the data aggregation market. Such a rulemaking would increase consumer protection and give the CFPB the authority to directly supervise and examine those entities for compliance with applicable data security standards and Federal consumer financial laws, including GLBA, just as banks are regularly examined for compliance with the GLBA's information security standards and Federal consumer financial laws. The FFIEC exam 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.[29] A larger market participant rulemaking for this market also would enable the CFPB to supervise and examine those participants for compliance with the final rules the CFPB issues under Section 1033 of the Dodd-Frank Act as well as identify and address risks as part of the supervisory process prior to significant consumer harm. Further, information gained as part of a comprehensive supervisory approach can better inform future CFPB actions to protect consumers in the data aggregation marketplace.

Conclusion and recommendation

To protect consumers and ensure that privacy and cyber risks are managed appropriately, all participants in the consumer data sharing ecosystem with access to consumer data should be subject to the same requirements and oversight for their privacy and security practices. Without these protections, U.S. consumers' information and financial health could be put at risk.

A larger market participant rulemaking would give the CFPB the authority to supervise and examine data aggregators and other relevant entities in the consumer data sharing ecosystem posing the highest risk to consumers for compliance with applicable data security standards and Federal consumer financial laws, just as banks are regularly examined for compliance with the GLBA's information security standards, agency guidance, and consumer financial protection laws. Identifying

[27] CFPB Consumer Financial Protection Circular 2022-04, "Insufficient data protection or security for sensitive consumer information," (August 11, 2022), available at: Consumer Financial Protection Circular 2022 04 Insufficient data protection or security for sensitive consumer information (consumerfinance.gov).

[28] See, e.g., CFPB, *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation* (October 18, 2017), available at: cfpb_consumer-protection-principles_data-aggregation.pdf (consumerfinance.gov); Advance Notice of Proposed Rulemaking issued by the Consumer Financial Protection Bureau seeking input on consumers access to financial records pursuant to Section 1033 of the Dodd-Frank Act. 85 Fed. Reg. 71003 (Nov. 6, 2020).

[29] FFIEC, Information Technology Examination Handbook, Information Security Booklet, available at: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx

and addressing consumer risk through supervision will allow for a timelier resolution of issues and thus reduce overall consumer harm. CFPB supervisory and examination authority over data aggregators and data users would further enhance the movement towards greater consumer data security by enabling the CFPB to have direct oversight of data aggregators' and data users' data security and cybersecurity practices.

* * * * *

If you have any questions, please contact the undersigned by phone at 703-887-5229 or by email at paige.paridon@bpi.com.

Sincerely,

Paige P. Paridon

Paige Pidano Paridon
Senior Vice President,
Senior Associate General Counsel
Bank Policy Institute