UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY
LEXINGTON DIVISION

FORCHT BANK, N.A., KENTUCKY BANKERS ASSOCIATION, and BANK POLICY INSTITUTE, *Plaintiffs* v. CONSUMER FINANCIAL PROTECTION BUREAU and RUSSELL VOUGHT, in his official capacity *Defendants,* and FINANCIAL TECHNOLOGY ASSOCIATION, *Intervenor-Defendant*	)	No. 5-24-cv-304-DCR

MEMORANDUM OF THE FINANCIAL HEALTH NETWORK, CONSUMERS REPORTS, AND SAVERLIFE AS *AMICI CURIAE* IN SUPPORT OF INTERVENOR'S MOTION FOR SUMMARY JUDGMENT

Table of Contents

This Memorandum is submitted on behalf of the Financial Health Network, Consumers Union, and SaverLife as *amici curiae* in support of intervenor Financial Technology Association's opposition to plaintiffs' and defendants' motions for summary judgment and in support of intervenor's cross-motion. *Amici* are non-profit organizations dedicated to advancing the financial health of American households. The interests of the *amici* are set forth more fully in their accompany motion for leave to file this memorandum.

INTRODUCTION

Until the plaintiffs in this case filed their complaint, *amici*—who had participated in and closely followed the rulemaking process that led to the promulgation of the Personnel Financial Data Rights Rule at issue here—believed that one issue on which there was widespread consensus was that § 1033 of the Consumer Financial Protection Act of 2010 (CFPA), 12 U.S.C. § 5533, confers on consumers both the right to access their financial data directly as individuals and also the right to authorize third parties to do so on their behalf. That seemed clear from the language of § 1033 which requires access to data "in an electronic form usable by consumers" and directs the Consumer Financial Protection Bureau (CFPB or the Bureau), in issuing implementing regulations, to "promote the development and use of standardized formats…through the use of machine readable files." And, that seemed clear, as well, from the Act's definition of "consumer" as "an individual or an agent, trustee, or representative acting on behalf of an individual." 12 U.S.C. § 581(4).

Further, since the day that the CFPA took effect and the CFPB opened its doors, the term "consumer" has been understood to encompass anyone authorized by an individual to act on the individual's behalf, and not just those with a "special, fiduciary-like relationship

with the consumer" as plaintiffs and defendants now argue.[1] Thus, the Bureau's process for handling consumer complaints—a process required by § 1034 of the CFPA, 12 U.S.C. § 5534 –since the first has been open to complaints filed on behalf of an aggrieved individuals so long as the person submitting a complaint has been authorized by the aggrieved person to do so.[2] Since 2011, financial institutions--including, we believe, every member of plaintiff Bank Policy Institute (BPI) that offers consumer financial products and services--routinely have responded to complaints from such representatives in the same way that they have responded to complaints submitted directly by an aggrieved individual.

Moreover, both prior to and throughout the data rights rulemaking, parties of all political persuasions expressed a shared understanding that the CFPA empowers individual consumers to authorize third parties to access financial data on their behalf. For example, in 2016 then-CFPB Director Cordray, who had been appointed by President Obama, stated, "We believe consumers should be able to access [account] information and give their permission for third-party companies to access this information as well."[3] In 2018, the Treasury Department, in a report to President Trump, expressed the very same view, stating that the definition of consumer in the CFPA "is best interpreted to cover circumstances in which consumers affirmatively authorize, with adequate disclosure, third parties…to access

---

[1] Plaintiffs' Brief in Support of Their Motion for Summary Judgment at 17 (hereinafter Pl. Br.); *see* Defendants' Memorandum in Support of Their Motion for Summary Judgment at 9 (hereinafter Def. Mem.). For convenience, we use the term "plaintiffs" to refer to both plaintiffs and defendants except where expressly noted otherwise.

[2] *See, e.g.*, 76 Fed. Reg. 76628, 76631 (Dec. 11, 2011) (proposed policy on disclosure of complaints); 77 Fed. Reg. 37558, 37567 (June 12, 2012) (final policy on disclosure of complaints). Thus, insofar as § 1033's "neighboring provisions" are relevant here as plaintiffs posit, Pl. Mem. at 14, § 1034 undermines, rather than supports, plaintiffs' argument here.

[3] Prepared Remarks of CFPB Director Richard Cordray at Money 20/20 (Oct. 23, 2016), *available at* https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-cfpb-director-richard-cordray-money-2020/

their financial account and transaction data" and "recommend[ing] that the Bureau affirm that for the purposes of Section 1033 third parties properly authorized by consumers…fall within the definition of consumer."[4] And, in a comment submitted to the CFPB during the rulemaking process, the Chairman of the House Financial Services Committee, Patrick McHenry, also embraced this view.[5]

Perhaps most tellingly, this had been the consistent position of plaintiff Bank Policy Institute (BPI) until it filed the complaint in this case. For example, in congressional testimony in 2021, BPI "support[ed] the ability of bank customers to securely connect their bank accounts to third party apps of their choice" and BPI urged the Bureau, in "implementing section 1033 of the Dodd-Frank Act," which BPI recognized "provides the CFPB with authority to promulgate rules around consumer financial data sharing," to adopt a rule that "would accelerate the migration of consumer data sharing to [Application Programming Interfaces or] APIs."[6] (As we explain in Part III, that is precisely what the Rule at issue here does.) In responding to the CFPB's Advance Notice of Proposed Rulemaking BPI reiterated its belief that "consumers must have the ability to grant consent to share their financial data for services or applications."[7] And, in the comment it submitted to the CFPB on the proposed data rights rule, BPI expressly endorsed the CFPB's proposal to require data

---

[4] Treasury Department, *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation* at 31 (2018), *available at* *https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf*

[5] Letter from Chairman Patrick McHenry to Director Rohit Chopra on the Notice of Proposed Rulemaking (Dec. 13, 2023), *available at* *https://financialservices.house.gov/uploadedfiles/2023-12-12_1033_letter_12.12.2023_final.pdf*

[6] Statement by the Bank Policy Institute Before the U.S. House Committee on Financial Services Task Force on Financial Technology (Sept. 21, 2021), *available at* https://bpi.com/bpi-statement-before-house-task-force-on-financial-technology-on-consumer-consumers-access-to-personal-financial-data/

[7] BPI Response to CFPB Advance Notice of Proposed Rulemaking on Consumer Access to Financial Records at 8 (Feb. 4,2021)(), *available at* *https://www.regulations.gov/comment/CFPB-2020-0034-0026*.

providers—the phrase used to refer to financial institutions holding account and transactional data--to establish a "developer interface" for use by authorized third party representatives to access data on behalf of consumers stating:

> Proposed § 1033.201(a) would require a data provider to make available to a consumer *and an authorized third party,* upon request, covered data in the data provider's control or possession concerning a covered consumer financial product or service that the consumer obtained from the data provider. The CFPB requests comment on whether it would be clearer to interpret CFPA section 1033(a) to set forth certain explicit prohibitions against practices that might make data unavailable or unusable.
>
> *We generally support the proposed formulation* and do not believe that particular prohibitions are necessary. [Emphasis added] [8]

Indeed, in its comment letter—as in its prior statements—BPI effectively urged the CFPB to establish an exclusive means through which authorized third parties could access consumers' data by prohibiting such parties from using consumers' account login credentials (i.e., username and password) to log into a consumer's online account and "scrape" the information visible on the account portal.[9]

BPI, joined by Forcht Bank and the Kentucky Bankers Association (neither of which participated in the rulemaking process) and—remarkably enough—by the CFPB itself have now taken a U-turn and claim that the CFPB acted unlawfully in requiring data providers to provide direct data access to an individual's "authorized representative" as defined and

---

[8] Bank Policy Institute and The Clearinghouse Comment on Notice of Proposed Rulemaking on Personal Financial Data Rights at 38, (Dec. 29, 2023), *available at* https://www.regulations.gov/comment/CFPB-2023-0052-0918

[9] Paradoxically, although claiming that the CFPB lacks the authority to mandate data access to authorized third parties, plaintiffs (although not defendants) also contend that the CFPB acted arbitrarily by failing to prohibit authorized third parties from engaging in screen scraping. But the CFPB clearly explained its reason for concluding that such a prohibition was "unnecessary" in light of the restrictions the Rule places on third parties, restrictions that third parties "could not feasibly meet through screen scraping." 89 Fed. Reg. 90838, 90923 (Nov. 18, 2024). And, the CFPB "caution[ed]" that "Once data providers have enabled the…data access envisioned by the Rule, screen scraping attempts by third parties…could well be limited by the CFPA's prohibition on unfair, deceptive, and abusive acts and practices." *Id*.

delimited by the Rule. In plaintiffs' view, although § 1033 requires that data be made available "in an electronic format usable by consumers," the only way individual consumers can actually put their data to use is by downloading it and then uploading it to a third party; authorized representatives (other than those with a fiduciary-like relationship) can obtain data directly from the data provider only at the sufferance of the data provider. In this view, even if an individual authorizes a third party to access the individual's data to deliver a product or service desired by the individual—and even if, as is true under the Rule, the third party can only collect, use, and retain data needed to deliver that product or service-- the data provider is free to determine what data (if any) it will share with the authorized representative and under what terms and conditions--including whatever price the data provider may elect to charge.

Intervenor Financial Technology Association's (FTA) brief shows why plaintiffs' cramped reading of the phrase "agent, trustee, or representative acting on behalf of an individual" must fail as a matter of statutory interpretation. *Amici*, as non-profit organizations focused on advancing consumers' financial health, submit this Memorandum to demonstrate the extent to which consumers have come to rely on products and services provided by "fintech apps" to help them manage their financial lives, and how such apps use consumers' financial data, accessed with the express authorization of consumers, to deliver these products and services. As we further show, interpreting Section 1033 to apply only to direct individual access would, in the words of the Treasury Department's 2018 report, "eliminat[e] many of the benefits [consumers] derive from data aggregation and the

innovations that flow through from fintech applications."[10] Accordingly, we urge the Court to embrace the interpretation of the definition of "consumer" put forward by Intervenor—and at least implicitly agreed to by BPI and its member banks during the rulemaking process—and hold that authorized third parties as defined in the Rule are "agents" or "representatives" acting on "behalf of an individual" and thus covered by § 1033.

I. CONSUMERS REGULARLY AUTHORIZE TRUSTED THIRD PARTIES TO ACT ON THEIR BEHALF IN ACCESSING THEIR FINANCIAL DATA AS NEEDED TO DELIVER PRODUCTS AND SERVICES THAT ENABLE CONSUMERS TO MANAGE THEIR FINANCIAL LIVES MORE EFFECTIVELY

The digitization of commerce, coupled with the explosive growth in smartphones and other Internet access devices, have fundamentally transformed the types of financial services available to consumers as well as the way in which many consumers access financial services. The CFPB estimated that as of 2022, at least 100 million consumers had authorized a third party to access account and transaction data regarding their financial accounts and that the number of individual instances in which such authorized third parties accessed, or attempted to access data, exceeded 50 billion and may have been as high as 100 billion. 89 Fed. Reg. 90838, 90840 (Nov.18,2024). These third parties use the data they obtain with consumers' authorization to deliver products and services requested by the consumer to assist them in managing their financial lives. We describe below some of the leading examples of fintech apps using such consumer-permissioned data and the difference these apps can make, and are making, in consumers' financial lives. (We use the term "fintech app" in its broadest sense to refer to any application that receives and analyzes

[10] Treasury Department, *supra* n. 4.

data in an electronic format in connection with the delivery of a consumer financial product or service; such apps may be—and are--provided by mainstream financial institutions such as banks and credit unions, by so-called fintech companies, and by non-profit organizations like certain of the *amici*.)

Facilitating person-to-person (P2P) payments: Probably the most commonly used fintech apps are those like PayPal, Venmo, or CashApp that enable consumers to send money to one another seamlessly. These apps make it easier, quicker, and less costly for consumers to pay for a shared cost, such as rent, utility bills, or a restaurant bill. The apps also make it easier for individuals to lend or give money to a friend or family member or to pay (and get paid) for personal services like babysitting, dog walking and the like.

A key feature of these P2P apps is that consumers can send money to other members of the network in real time without having to wait for a check or ACH payment to settle and clear and without having to keep money in reserve in their P2P account. This is an especially important feature for the millions of Americans living paycheck to paycheck who may need to turn to friends and family for money in an emergency or who may need to make a last-minute payment but who cannot afford to keep money in reserve.

To make these real-time payments possible, consumers link their P2P accounts with a funding mechanism, typically a checking account, and authorize the app to access account balance information so that, when a consumer requests the app to send money, the app can check the account balance to verify that the consumer will be able to fund the transaction. The consumer also typically authorizes the app to access the consumer's payment initiation information—typically the account and routing number—so that the app

can initiate an electronic debit from the consumer's checking account to cover the transaction. (This makes it easier for consumers to sign up for the app because they do not have to enter that information directly into the app as part of the enrollment process.)

Broadening access to credit: In today's economy, access to credit is essential to finance major expenses such as the purchase of a home, an automobile, or other consumer durables. For the over forty percent of Americans with under $1,000 in savings, credit is equally vital to enable them to withstand financial shocks, such as a loss of income or a major expense.[11] But to obtain credit from a bank, credit union, or finance company a consumer generally must have a credit score which is generated from data contained in a credit report maintained by one of the three national credit bureaus.[12] This creates a classic Catch 22 for the estimated 25,000,000 Americans who either do not have a credit report or whose credit report has too little current information to generate a reliable score.[13] Because these consumers lack sufficient credit history, they are severely hindered in their ability to obtain credit (and build such history). This means that those most in need of credit—low and moderate income consumers -- experience the greatest difficulty obtaining it.

Even for those with a scorable credit report, their credit score may understate their creditworthiness, *i.e.,* their ability to repay a new loan, and thus hinder their ability to obtain

---

[11] *See* Board of Governors of the Federal Reserve System, *Economic Well-Being of U.S. Households in 2024* at 42 (May 2025), *available at* https://www.federalreserve.gov/publications/files/2024-report-economic-well-being-us-households-202505.pdf

[12] As a formal legal matter, the reports from which credit scores are generated are considered "consumer reports" and the national organizations maintaining those reports "national consumer reporting agencies," *see* 15 U.S.C. § 1681(d), (f),(p), but in practice virtually all the information contained in such reports come from creditors.

[13] Kambara & Luce, *Technical correction and update to the CFPB's credit invisibles estimate* (CFPB 2025), *available at* https://files.consumerfinance.gov/f/documents/cfpb_update-credit-invisibles-estimate_2025-06.pdf. This study finds that 12.5% of Americans lack a credit score; that translates to roughly 25 million individuals.

credit on affordable terms. This is true for two reasons. First, consumers who experienced financial difficulty in the past may find their scores depressed long after they have recovered from the difficulty because negative information generally is retained in a credit report for seven years (or in some cases even longer). Second, consumers who are relatively new to credit may find their scores depressed by the very thinness of their credit history which makes it harder to predict their likelihood of defaulting on a new loan.

A wealth of recent research has demonstrated that transactional data from consumers' checking accounts can mitigate these limitations of the credit reporting and scoring system. Transactional data reflects consumers' current cash inflows and outflows and thus provides a more current picture of a consumer's financial situation than a traditional credit report. Further, by analyzing transactional data over time it is possible to identify payments for recurring obligations—for example, monthly rent, utility, and telecommunication payments—that generally are not reflected in traditional credit reports but that have been proven to be indicative of a consumer's creditworthiness.[14]

In light of this research several fintech apps—including one offered by Experian, one of the national credit bureaus,[15] and one offered by FICO, the developer of the most widely-

[14] *See, e.g.,* FinReg Lab, *The Use of Cash Flow Data in Underwriting Credit: Empirical Research Findings, Technical Report* (2019), *available at* https://finreglab.org/wp-content/uploads/2023/12/FinRegLab_2019-07-25_Research-Report_The-Use-of-Cash-Flow-Data-in-Underwriting-Credit_Empirical-Research-Findings.pdf ; Alexandrov, Brown & Jain, *Looking at credit scores only tells part of the story—cashflow data may tell another part* (CFPB, 2023), *available at* https://www.consumerfinance.gov/about-us/blog/credit-scores-only-tells-part-of-the-story-cashflow-data/ ; Johnson, *Everything You Ever Wanted to Know About Cash Flow Underwriting But Were Afraid to Ask* (Fintech Takes, May 22, 2024), *available at* https://fintechtakes.com/articles/2024-05-22/cash-flow-underwriting/

[15] https://www.experian.com/credit/score-boost/

used credit scoring algorithm,[16] as well as apps provided by various fintechs[17]—enable consumers to authorize access to data from their checking accounts. With this authorization, the apps can obtain consumers' transactional data, identify specified types of recurring bill payments, and feed that information into the consumer's credit report to generate, or enhance the predictiveness of, a credit score. The apps do so on an ongoing basis, providing an opportunity for consumers to keep expanding their payment history.

Beyond this, multiple lenders now engage in "cash flow underwriting" either as a complement to, or as a substitute for, basing their underwriting decisions on a credit score. Consumers seeking loans from these lenders are invited to authorize the lender to access the consumer's transactional data history from their bank, on the consumer's behalf, to assess the consumer's ability to repay a potential loan. Using these data, lenders are able to assess creditworthiness based on what the data shows regarding the consumer's cash inflows and outflows and repayment history.[18] Such cash flow underwriting, coupled with authorized access to the consumer's payment initiation information, has enabled some lenders to introduce new types of credit products—such as short-term, no-interest cash advances—in which the loan proceeds are directly deposited into the consumer's checking account and the loan payment debited from that account when due.[19] Other lenders use

---

[16] https://www.fico.com/en/products/ultrafico-score

[17] For a compendium of some of these apps *see* Cochran & Stegman, *Utilities, Telecommunications, and Rental Data in Underwriting Credit* App. D (2022), *available at https://www.urban.org/sites/default/files/2022-06/utility-telecommunications-and-rental-data-in-underwriting-credit_0.pdf*

[18] There are now commercially-available cash flow scores including one recently launched by Experian, https://www.experianplc.com/newsroom/press-releases/2025/launch-of-experian-s-cashflow-score-signals-new-era-of-open-bank as well as cashflow scores from , Prism Data, https://prismdata.com/cashscore/, and Nova Credit, https://www.novacredit.com/novascore

[19] Examples include Dave ExtraCash, https://dave.com/about-extra-cash, Money Lion InstaCash, https://www.moneylion.com/cash-advance/instacash, and Earnin Cash Advance, https://www.earnin.com/

consumer-permissioned cash flow data to underwrite for more conventional credit products such as credit cards and auto and personal loans; indeed, since 2020, over three successive Administrations, the Office of the Comptroller of the Currency has been working with financial institutions to enhance financial inclusion through cash flow underwriting.[20]

Assistance with personal financial management: For all its advantages, the digital age has made it more complicated for consumers to manage their day-to-day finances. There was a time, not so very long ago, when consumers deposited their paychecks each payday at their local bank, withdrew cash to make day-to-day purchases, wrote checks to pay their monthly bills, and maintained a running balance in their check register in which they entered each deposit, withdrawal, and check. That is no longer feasible, as money flows into checking accounts electronically and flows out electronically multiple times each day through the use of debit cards, mobile wallets like Apple Pay or Google Pay, P2P apps, automated bill payments, and the like. Keeping track of when and where money is going, and how much is available to spend without incurring an overdraft or nonsufficient funds fee, is increasingly challenging for many consumers especially since different types of transactions take different times to settle and clear depending on, *e.g.,* the mode of payment and the speed with which the payee initiates the process of obtaining payment.

These challenges weigh especially heavily on the tens of millions of consumers who are living financially precarious lives. The Federal Reserve Board recently found that 27% of Americans are "just getting by" or "finding it difficult to get by"; a comparable percentage

[20] *See, e.g.,* OCC, *Project REACh Alternative Credit Assessment Workstream,* *https://www.occ.treas.gov/topics/consumers-and-communities/project-reach/alternative-credit-assessment-workstream.html*

reported skipping needed health care in the prior year due to the cost; and an even higher percentage reported that they could not handle an emergency expense above $500.[21] These consumers have limited bandwidth to deal with their finances yet, at the same time, little if any slack in their budgets and hence a greater need to stay on top of their finances.

Numerous "personal financial management" apps have emerged to help consumers address these challenges. The common denominator across these apps is that consumers who elect to use them authorize the app to obtain transactional and account data—often across multiple accounts including checking, savings, and credit cards accounts-- on an ongoing basis to deliver ongoing services. With these data, and utilizing sophisticated algorithms and, increasingly, artificial intelligence, the apps provide a wide range of tools and services. Some apps, for example, identify recurring monthly or annual debits for subscription services that the consumer may no longer be using but has not canceled. Other apps track expenses in defined categories and help consumers establish, and adhere to, a family budget. Still other apps alert consumers to upcoming expenses such as automated debits and advise consumers of how much of a current checking account balance is safe to spend or when the consumer needs to move money into their account (or reduce spending) to cover a forthcoming expense without overdrafting. Savings apps advise consumers when there is "extra" money in an account that can safely be moved into an emergency savings account and, with the consumer's authorization, can even execute such transactions by using the consumer's payment initiation information to withdraw money. And, many

[21] Federal Reserve Board, *supra* n.4, at 5,38,42.

personal financial management apps provide customized financial advice as to ways consumers can optimize or even reduce their spending and increase their savings.[22]

These are only some of the services that personal finance management apps provide today. Importantly, all these services depend on the apps' ability to regularly access, ingest, and analyze data from the consumer's accounts. And as advances in artificial intelligence unlock new ways to analyze data and assist consumers in managing their financial lives the list of services available to consumers—and the ongoing need to access consumer-permissioned data—will only continue to grow.

In sum, as the 2018 Treasury Department report concluded, the ability of consumers to authorize third parties to access their account and transactional data, and the fintech apps that use these data, have "exponentially improved a consumer's ability to make financial decisions" while expanding financial inclusion.[23]

We pause to add one additional point. As the foregoing indicates, many of these fintech apps use consumers' payment initiation information to deliver the services consumers request, for example to repay a P2P advance, disburse a loan, or automate savings. Plaintiffs (although not defendants) claim that the CFPB acted unlawfully in requiring data providers to allow access to such information. As Intervenor shows, that argument runs contrary to both the broad grant of rulemaking authority contained in § 1033

---

[22] For a listing of a small sampling of these apps *see, e.g.,* Purdue Global, *26 Personal Finance Tools, Apps, and Resources for College Students* (2025), *available at* https://www.purdueglobal.edu/blog/student-life/budgeting-apps-personal-finance-tools/; Bending, *Best Budgeting Apps of 2025* (Forbes, June 16, 2025), *available at* https://www.forbes.com/advisor/banking/best-budgeting-apps/ ; Egan, *Automatic Savings Apps for the Forgetful* (US News Jan. 28, 2025), https://www.usnews.com/banking/articles/automatic-money-saving-apps-for-the-forgetful.

[23] Treasury Department, *supra* n. 4, at 22.

as well as the explicit language entitling consumers and their representative access to "information relating to…the account." Beyond that, we note that although plaintiffs assert that this requirement "creates significantly enhanced risk of compromise of such data, and thus consumers' funds," Pl. Mem. at 22, precisely the opposite is true. The Rule permits data providers to limit access to a "tokenized" (i.e., encrypted) version of payment initiation information. 12 C.F.R. § 1033.211(c). Absent that provision, consumers desiring fintech apps to initiate payments would be required to manually provide their account and routing numbers—as consumers are legally entitled to do and do all the time in authorizing electronic debits; this would pose more risk to consumers than that posed by access to tokenized information under the Rule.

II. THE CFPB'S PERSONAL FINANCIAL DATA RIGHTS RULE CEMENTS THE ROLE OF FINTECH APPS AS AGENTS OR REPRESENTATIVES ACTING ON BEHALF OF THE INDIVIDUALS WHO AUTHORIZE ACCESS TO THEIR DATA AND ADDS IMPORTANT PROTECTIONS TO SUCH INDIVIDUAL CONSUMERS.

As the foregoing discussion makes plain, the fintech apps that access financial data stand in the shoes of the individuals whose data they access. They can do so only with the express authorization of such individuals which these consumers provide to obtain services from the fintech apps. For those reasons alone, in accessing such data these apps squarely meet the statutory definition of "consumer" because they are either "agents" or "representatives acting on behalf of an individual."

Moreover, under the terms of the Rule, for a fintech app to qualify as an "authorized third party" and be entitled to obtain consumers' account data, the app must abide by a set of requirements that further assure--if there were any room for doubt—that such apps are

acting on behalf of, and for the benefit of, the consumers. To begin with, an authorized third party is defined as one who has obtained a signed "authorization disclosure" containing the consumer's "express informed consent" permitting the third party to "access covered data on behalf of the consumer." 12 C.F.R. § 1033.131. The authorization disclosure must identify the data provider (*i.e.*, the financial institution) from whom data is to be obtained, the product or service to be provided to the consumer for which the data is to be obtained, and the "categories of data that will be accessed." *Id*. *s*§ 1033.411(b). Before providing access to data, the data provider is entitled to confirm with the consumer the scope of the third party's authorization to access the consumer's data. *Id*. § 1033.331(b)((2).

Further, under the terms of the Rule, an authorized third party can only collect such data as is "reasonably necessary to provide the consumer's requested product or service." *Id*. § 1033.421(a)(1). An authorized third party likewise can only use the data for the purpose of providing such product or service. *Id*. And, if the consumer revokes the authorization, which the consumer can do at will, or if the authorization expires and is not renewed which must occur at least annually, the third party must cease collecting new data, or using or retaining existing data, unless doing so is "necessary to provide the consumer's requested product or service." *Id*. § 1033.421(a(1). All these obligations—along with an obligation placed upon an authorized third party to establish a legally sufficient information security program, *id*. § 1033.421(e)--are set forth in a provision of the Rule entitled "Third party obligations" and thus are directly enforceable by the CFPB. (Plaintiffs' claim that the Bureau

"refused to assume any clear role in ensuring that third parties comply with the Rule, Pl. Mem. at 23, is thus wide of the mark.[24])

Plaintiffs (but not defendants) contend that the fact that the Rule permits authorized third parties to retain a data aggregator to mechanically access data somehow indicates that such third parties are not acting as agents or representatives of the consumer. Pl. Mem. at 17-18. Data aggregators play an important role in the data sharing ecosystem because they have developed the technology and relationships required to access data from thousands of banks and credit unions so that each third party does not have to separately do so; data providers benefit as well by dealing with a small number of aggregators rather than thousands of authorized third parties. But the fact that authorized third parties use data aggregators to access data in no way detracts from the fact that the data is being accessed with the consumer's authorization and for the consumer's benefit. And, here, too, the Rule assures that this is so by requiring that if an authorized third party retains a data aggregator, the authorization disclosure which the consumer signs must identify the aggregator, and the aggregator must certify to the consumer that it will abide by the same restrictions on the collection, use, and retention of data that apply to the authorized third party.[25]

---

[24] Plaintiffs' suggestion that the CFPB arbitrarily placed the burden to "police the third parties" on data providers, Pl. Mem. at 23, is equally misplaced. The Bureau made explicit more than once that the Rule "does not require data providers to vet third parties," 89 Fed. Reg. at 90900; *see id*. at 90899. Nor is there any merit to plaintiffs' argument that the CFPB arbitrarily restricted banks' "core risk-management functions," Pl. Mem. at 26-29, since the Rule allows banks to vet requests for third parties for data access to assure that the third parties meet the requirements to be an "authorized third party" including the Rule's information security provision, and the Rule also permits banks to deny access to a third party based on a "specific risk of which the data provider is aware" that implicates safety and soundness concerns, *see* 12 C,.F.R. § 1033.321.

[25] *Id*. §§ 1033.131 (definition of "data aggregator"), 1033. 431. The same restrictions apply with respect to any subcontractor retained by an authorized third party to deliver to consumers the services requested by such consumers. *Id*. § 1033.421(f). These limitations parallel the obligations of sub-agents under the law of agency. *See generally* Restatement (3rd) of Agency § 3.15.

Defendants advance a different argument in claiming that authorized third parties are not agents or representatives acting on behalf of consumers: defendants argue that because the Rule permits an authorized third party to use data as "reasonably necessary to improve the product or service the consumer requested," 12 C.F.R. § 1033.411(c)(4), this somehow indicates that authorized third parties are not acting "on behalf of" the consumer. But as the CFPB observed in adopting this provision, consumers who request a product or service from a fintech app want the very best version of that product or service that the app can deliver, and thus permitting data to be used for product or improvements hardly suggests that the fintech app is not acting on the consumer's behalf. 89 Fed. Reg. at 90940-41. Indeed, the fact that, despite the urging of many commenters including some of the *amici*, the Rule prohibits an authorized third party from using consumers' data to develop new products, or to identify existing products that might also benefit a given consumer—and does not even permit consumers to opt in to authorize such "secondary uses"--makes plain the pains that the Bureau took, in crafting the Rule, to assure that authorized third parties satisfy the statutory definition of a "consumer."[26]

In short, both the inherent nature of the relationship between fintech apps and the consumers who authorize such apps to access their account data as well as the specific provisions of the CFPB rule assure that those fintech apps that qualify as "authorized third parties" are acting "on behalf of the consumer" as the consumer's "agent" or "representative" in accessing such data.

[26] *See* 12 C.F.R. § 1033.421(a)(2) (prohibiting use of covered data for targeted advertising and cross-selling); 89 Fed. Reg. at 90941 (rejecting proposals to permit opt-in because of concerns that consumers about "meaningful consent"), 90973 (noting prohibition on using data for new product development).

We pause once again to make one additional point. Plaintiffs assert that because § 1033 is silent with respect to the subject of fees, the CFPB exceeded its statutory authority in prohibiting data providers from charging authorized third parties a fee to access consumer data. But given that "[s]ubject to rules prescribed by the Bureau" § 1033 requires data providers to make account and transactional data available to consumers—and given that, as we have shown, the term "consumer" includes authorized representatives as defined in the Rule—the CFPB was surely within its rights to bar data providers from charging a fee when consumers exercise their statutory right. Indeed, as Intervenor argues, if anything the CFPB would have exceeded its authority had it permitted data holders to charge fees or, as defendants suggest, Def, Mem. at 12, to determine what fees are "reasonable."[27]

III. THE BENEFITS CONSUMERS ARE DERIVING, AND STAND TO DERIVE UNDER THE RULE, THROUGH PERMISSIONING ACCESS TO THEIR DATA WOULD BE SEVERELY THREATENED IF AUTHORIZED THIRD PARTIES WERE EXCLUDED FROM THE REACH OF SECTION 1033.

As the discussion in Part I shows, consumers are benefiting in multiple ways by authorizing third parties to access their account and transaction data. As Part II demonstrates, the Rule would further empower consumers by ensuring that when individuals grant such authorization they do so on an informed basis and that the authorized third are limited in the data they can access and the purposes for which, and period during which, those data can be used and retained. Plaintiffs' attack on the Rule would strip consumers of the protections that the Rule—and the statute--would afford. As the Treasury

[27] Plaintiffs' argument that explicit authority is required to justify the fee prohibition in the Rule is especially startling in light of the multiple other provisions plaintiffs claim the CFPB should have adopted, all without explicit statutory authority including, e.g., a provision allocating liability for data compromise, Pl. Mem. at 29-31, or a provision prohibiting screen scraping, *id*. at 24.

Department warned, this "would … eliminat[e] many of the benefits [consumers] derive from data aggregation and the innovations that flow through from fintech applications."[28] To explain why that is so, it is necessary to explore how data access functions today to understand how that could change if authorized third parties could access data only at the sufferance of banks and other data providers.

As the CFPB observed in proposing the Rule, third party access is generally enabled by one of two methods: through "screen scraping" or through "developer interfaces." In screen scraping individuals seeking a product or service from a third party share their login credentials for their online or mobile banking portal (i.e., their username and password) with the third party's aggregator. The aggregator then uses those credentials to log into the consumer's account, capture the information displayed on the portal, and convert that information into standardized, machine-readable data that can be used by the third party to deliver to the consumer the requested product or service. Developer interfaces, in contrast, are maintained by financial institutions that hold financial account data (i.e., data providers) typically through APIs; these APIs can be accessed only with secure credentials and they enable the direct transmission of structured, machine-readable data from the data provider to an authorized third party, typically through an aggregator, pursuant to bilateral agreements between the data provider and the aggregator. 88 Fed. Reg. 74796, 74798 (Oct. 31, 2023).

APIs have multiple advantages over screen scraping as a means of accessing consumer-permissioned data. First, APIs are more reliable; when screen scraping was the dominant mode of data access, third parties seeking to access data were unsuccessful

[28] Treasury, *supra* n. 4 at 31.

between 40% and 50% of the time.[29] Second, by providing structured data directly from the data provider, APIs reduce the risk of inaccuracies in the data that is obtained. Third, APIs protect consumers' privacy by limiting the data that third parties, or their aggregators, can access to only those data elements that are needed to deliver a particular product or service; in contrast, with screen scraping the aggregator necessarily pulls all the data on the screen even if the third party only needs a subset of such data, as, for example, when a P2P app needs to verify a current account balance. Fourth and finally, APIs reduce the risk—both to consumers and to financial institutions--of security breaches because with APIs neither third parties nor aggregators need to access or store consumers' login credentials. As a result, if there were to be a data breach at a third party or aggregator, consumers' usernames and passwords would not be exposed and subjected to misuse.

For all these reasons there is, as the CFPB also stated in proposing the Rule, "nearly universal consensus that developer interfaces should supplant screen scraping. 88 Fed. Reg. at 74798. But notwithstanding that agreement, the process of transitioning from screen scraping—which, in 2010, when the CFPA was enacted, was the dominant form of data access--to APIs has proved to be painstakingly slow. The first protocol for a data access API was released in 1997 by a three-company consortium and in 2015 that consortium was relaunched with a broader set of industry representatives.[30] Yet in the proposed rule the CFPB estimated that as recently as 2021, most access was still occurring via screen

---

[29] Written Submission of Steven Boms on Behalf of the Financial Data and Technology Association of North America to the CFPB Symposium on Consumer Access to Financial Records at 9 (Feb. 26,2020), *available at* https://files.consumerfinance.gov/f/documents/cfpb_boms-statement_symposium-consumer-access-financial-records.pdf.

[30] Plaid, *Financial Data Access Method: Creating a balanced approach* at 8 (2016), *available at* https://plaid.com/documents/Plaid-Financial-Data-Access-Methods.pdf .

scraping" and that even in 2023 only about half of third party data access occurred through APIs. 88 Fed. Reg. at 74798. Similarly, data from the Financial Data Exchange, the industry standard-setting body, indicates that as of the Spring of 2021 only 16 million accounts could be accessed via APIs; by April 2025 that number had increased to 114 million.[31]

Several factors help explain why progress was so slow at least until the CFPB began actively engaging in this data rights rulemaking. Although large financial institutions have been able to readily access the resources required to build APIs, for smaller institutions that has been more challenging. Further, connecting to an API generally has required the aggregator to agree to a data provider's terms of access, including agreeing with respect to what data elements can be accessed, with what frequency, and under what conditions. Some negotiations between financial institutions and third parties were reported to have dragged on for up to three years,[32] and at least one large bank reportedly attempted to restrict access to a single aggregator that was owned by a consortium of banks.[33] And, as the Treasury Department stated in its 2018 report, even after negotiating API agreements at least some aggregators found that, "access through APIs was frequently and unilaterally restricted, interrupted, or terminated by financial services companies."[34]

---

[31] Financial Data Exchange, *114 Million Reasons to Keep Moving Forward on Industry Led Standards for Secure Data Sharing* (April 25, 2025), *available at* https://www.financialdataexchange.org/FDX/News/Press-Releases/114%20Million%20Reasons%20to%20Keep%20Moving%20Forward%20on%20Industry-Led%20Standard%20for%20Secure%20Data%20Sharing.aspx.

[32] *See* Financial Data and Technology Association, *Response to the CFPB Advance Notice of Proposed Rulemaking Regarding Section 1033* (Feb. 3, 2021), *available at* https://www.regulations.gov/comment/CFPB-2016-0048-0034

[33] Johnson, *8 Questions About the Future of Open Banking* (Fintech Takes, Oct. 6,2023), *available at* https://fintechtakes.com/articles/2023-10-06/8-questions-open-banking/

[34] Treasury Department, *supra n.*4, at 27-28.

It was against this background that the CFPB, at the culmination of a process that began with the issuance of an Advance Notice of Proposed Rulemaking in 2020 and continued through the issuance of an Outline of Proposals and Alternatives Under Consideration in 2022 and a proposed rule in 2023, promulgated the Rule at issue here.[35] While exempting the over 7,500 depository institutions (banks and credit unions) that qualify as small businesses under standards established by the Small Business Administration, the Rule requires the remaining 1,665 depositories to establish, or if already established maintain, a "developer interface" or API through which a third party that qualifies as an authorized third party can access individuals' account and transactional data subject to the limitations on the collection, retention, and use of data discussed above.[36] The Rule further defines the data elements that must be accessible (referred to as "covered data") through the API, 12 C.F.R. § 1033.211, and prohibits the depositories from "unreasonably restrict[ing] the frequency with which it receives or responds to requests for covered data from an authorized third party," *id*. § 1033.311(d). In short, consistent with the statute, the Rule creates a regime in which individuals can authorize access to their financial data *as a matter of right* rather than one in which data access exists at the sufferance of the various financial institutions holding the data.

[35] The Advance Notice of Proposed Rulemaking can be found at 85 Fed. Reg. 71003 (Nov. 6,2020) and the proposed rule at 88 Fed. Reg. 74796 (Oct. 31, 2023); the Outline of Proposals and Alternatives—which was issued pursuant to the Small Business Enforcement and Fairness Act, 5 U.S.C. § 609-- is available at https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf.

[36] The exemption is set forth in 12 C.F.R. § 1033.111(d); *see* 89 Fed. Reg. at 90985 for the calculation of the number of exempt and covered depository institutions. The Rule also applies to an estimated 120 non-depositories providing covered products. *Id*.

The data rights regime that § 1033 and the Data Rights Rule are designed to establish would come undone if, as plaintiffs urge, the CFPA were interpreted to confer only a right of individual access and not a right of individuals to permission access by their authorized third party representatives. One immediate consequence of such a holding would be that the progress that has been made in transitioning away from screen scraping and towards API-based access would be stopped dead in its tracks, as those institutions that have not yet moved towards establishing an API—and that is still true of a large share of the institutions covered by the Rule--are unlikely to do so in the absence of a legal requirement. Beyond that, even where APIs exist today, stripping individuals of the right to permission access to their data would degrade and disrupt consumers' ability to do so and thus, to repeat Treasury's words, "eliminat[e] many of the benefits [consumers] derive from data aggregation and the innovations that flow through from fintech applications."

It is not difficult to understand the basis for Treasury's prediction. Section 1033 applies only to providers of consumer financial products and services, and outside that sphere some financial institutions have severely restricted their customers' ability to permission access to their financial data.[37] Further, at least until the § 1033 rulemaking gained a head of steam, several large banks attempted to do the same. Thus, if left free to preclude access by authorized third parties, some large banks might limit access to the one aggregator that they jointly own, giving that aggregator monopoly power. Banks could leave their APIs open to multiple aggregators but preclude access to certain apps, such as P2P

[37]Johnson, *8 Questions About the Future of Open Banking* (Fintech Takes, Oct. 6,2023), *available at* *https://fintechtakes.com/articles/2023-10-06/8-questions-open-banking/*

apps, in an attempt to drive traffic to a payment app (Zelle) which is also owned by a consortium of banks. Banks likewise could restrict access to certain apps, or certain data elements such as the pricing terms for accounts, to blunt price competition. Or banks could seek to monetize the consumers' data by treating their APIs as toll booths and imposing surcharges for accessing data. This is not merely a parade of hypothetical horribles; it is, rather, a list of actions that some banks have taken in the past and that would be in banks' interest to take if freed from any legal duty to allow data access to authorized third parties.[38]

To mitigate risks such as these, aggregators and fintech apps could revert to credential-based screen scraping as their primary means of accessing data because screen scraping, when successful, captures all data and not just those elements that a bank chooses to make available and can be effectuated without incurring a bank-imposed fee or securing a bank's permission. Such a reversion would make data access less dependable, the data that is accessed less accurate, and, most importantly, the process of accessing data less secure, potentially exposing millions of customers to heightened fraud risk.

---

[38] Johnson, *supra* n. 37; *PNC Blocks Venmo, Tells Users to Switch to Zelle* (PYMNTS, Dec. 16, 2019), *available at https://www.pymnts.com/news/mobile-payments/2019/venmo-claims-pnc-is-diverting-users-to-zelle/*. *See also* Sidel, *Big Banks Lock Horns with Personal Finance Web Portals* (Wall St. J., Nov. 4, 2015), *available at https://www.wsj.com/articles/big-banks-lock-horns-with-personal-finance-web-portals-1446683450*; Rudegair, *J.P. Morgan Warns It Could Unplug Quicken and Quickbook Users* (Wall St. J., Nov. 24, 2015), *available at https://www.wsj.com/articles/j-p-morgan-may-unplug-some-customers-access-to-account-data-1448375950*; Huang & Rudegair, *Bank of America Cut Off Finance Sites From Its Data* (Wall St. J., Nov, 9, 2015), https://www.wsj.com/articles/bank-of-america-cut-off-finance-sites-from-its-data-1447115089; Fintech Collective, *Capital One Restricts Third Party Access to Plaid, Upsets Customers* (June 29, 2018), *available at https://news.fintech.io/post/102ey7d/capital-one-restricts-third-party-data-access-to-plaid-upsets-customers: Written Testimony of MX Technologies, CFPB Symposium on Consumer Access to Financial Records* at 3 (Feb. 2, 2020), *available at https://files.consumerfinance.gov/f/documents/cfpb_barratt-statement_symposium-consumer-access-financial-records.pdf*

As Yogi Berra is reputed to have said, "it is tough to make predictions, especially about the future." Thus, we cannot claim to know precisely how banks and other data providers would respond if the phrase "representative acting on behalf of an individual" were interpreted as a legal term of art that excludes authorized third parties from the ambit of § 1033. But what is clear is that banks would have *carte blanche* to pursue their own self-interest in determining whether, when, and how much data to allow authorized third parties to access. And what is predictable, therefore, is that, to repeat Treasury's warning once more, the result of such an interpretation "would … eliminat[e] many of the benefits [consumers] derive from data aggregation and the innovations that flow through from fintech applications." The end losers, of course, would be the tens of millions of consumers who have come to rely on fintech-delivered products and services, and most especially those financially struggling consumers who turn to fintech apps to help them secure access to credit and manage their day to day financial lives.

CONCLUSION

For the foregoing reasons, and those set forth in the Memorandum of Intervenor in Support of its Motion for Summary Judgment, the motions of Plaintiffs and Defendants for summary judgment should be denied and the motion of Intervenor should be granted.

Respectfully submitted,

/s/ David M. Silberman _____

DAVID M. SILBERMAN (*pro hac vice)*
Financial Health Network
1140 Connecticut Ave NW Suite 920
Washington, DC 20036
(301) 943-1766
dsilberman@finhealthnetwork.org

JAMES CRAIG
The Craig Firm
Waterfront Plaza Building, Suite 1808
325 West Main Street
Louisville, KY 40202
(502) 544-5667
james@craigfirm.com

Counsel for amici curiae Financial Health Network, Consumer Reports, and SaverLife

CERTIFICATE OF SERVICE

I hereby certify that on this day I electronically filed the foregoing with the Clerk of the Court for the United States District Court for the Eastern District of Kentucky, Lexington Division, using the CM/ECF system, which will send a notice of filing to all counsel of record who have consented to service by electronic means.

Dated: July 4, 2025

/s/ James Craig
JAMES CRAIG