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

PLAINTIFFS' BRIEF IN SUPPORT OF THEIR MOTION FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

Page

PRELIMINARY STATEMENT 1

BACKGROUND 4

A. Open Banking 4

B. The Bureau's Rulemaking 7

C. The Bureau's Concession That The Rule Is Unlawful 11

STANDARD OF REVIEW 11

ARGUMENT 12

I. THE RULE EXCEEDS THE BUREAU'S STATUTORY AUTHORITY. 12

A. Section 1033 Does Not Authorize The Bureau To Compel Banks To Share Data With Commercial Third Parties (Count I). 13

1. "Consumer" In Section 1033 Means The Individual Consumer. 14

2. The General Definition Of "Consumer" In Section 1002 of Dodd-Frank Does Not Support The Rule. 15

B. Section 1033 Does Not Permit The Bureau To Enlist Private Standard-Setting Organizations To Set Compliance Standards (Count VI). 19

II. THE RULE'S MASS DATA-SHARING FRAMEWORK IS ARBITRARY AND CAPRICIOUS (COUNT II). 21

III. SEVERAL INDIVIDUAL FEATURES RENDER THE RULE UNLAWFUL. 24

A. Section 1033 Does Not Authorize The Bureau To Require Banks To Share Payment-Initiation Information (Count V). 25

B. The Rule's Restrictions On Banks' Core Risk-Management Functions Are Arbitrary And Capricious (Count III). 26

C. The Bureau's Refusal To Prescribe Rules Allocating Liability For Data Compromise Is Arbitrary And Capricious (Count IV). 29

D. The Bureau's Performance Standards For Developer Interfaces Are Unlawfully Vague (Count VII). 32

E. The Rule's Fixed Compliance Timeline Is Arbitrary And Capricious (Count VIII). 34

F. The Rule Unlawfully Prohibits Banks From Charging Fees For Access To The Developer Interfaces (Counts IX, X). 35

1. The Access-Fee Prohibition Exceeds The Bureau's Statutory Authority (Count IX). 36

2. The Access-Fee Ban Is Arbitrary And Capricious (Count X). 38

CONCLUSION 40

CERTIFICATE OF SERVICE 42

TABLE OF AUTHORITIES

Page(s)

Cases

Ala. Ass'n of Realtors v. *Dep't of Health & Human Servs.*,
594 U.S. 758 (2021) 37

Alliance for Hippocratic Med. v. *U.S. Food & Drug Admin.*,
78 F.4th 210 (5th Cir. 2023) 21

Am. Ass'n of Cosmetology Schools v. *Devos*,
258 F. Supp. 3d 50 (D.D.C. 2017) 21

Ass'n of Am. R.R. v. *U.S. Dep't of Transp.*,
721 F.3d 666 (D.C. Cir. 2013) 21, 34

Bond v. *United States*,
572 U.S. 844 (2014) 18

Brown v. *Gardner*,
513 U.S. 115 (1994) 14

Cincinnati Bell Telephone Co. v. *FCC*,
69 F.3d 752 (6th Cir. 1995) 38, 39

Consumers' Research v. *FCC*,
109 F.4th 743 (5th Cir. 2024) 19

Data Mktg. P'ship, LP v. *U.S. Dep't of Lab.*,
45 F.4th 846 (5th Cir. 2022) 12

Davenport v. *Lockwood, Andrews & Newnam, Inc.*,
854 F.3d 905 (6th Cir. 2017) 13

Dubin v. *United States*,
599 U.S. 110 (2023) 17

Envt'l Def. v. *Duke Energy Corp.*,
549 U.S. 561 (2007) 15

Evans v. *United States*,
504 U.S. 255 (1992) 16

Firearms Regulatory Accountability Coalition, Inc. v. *Garland*,
112 F.4th 507 (8th Cir. 2024) 32

Henson v. *Santander Consumer USA Inc.*,
582 U.S. 79 (2017) 15

Long Island Power Auth. v. *FERC*,
27 F.4th 705 (D.C. Cir. 2022) 12

Loper Bright Enters. v. *Raimondo*,
603 U.S. 369 (2024) 16

MCI WorldCom, Inc. v. *FCC*,
209 F.3d 760 (D.C. Cir. 2000) 35

Mich. First Credit Union v. *T-Mobile USA, Inc.*,
108 F.4th 421 (6th Cir. 2024) 30

Monroe Retail, Inc. v. *RBS Citizens, N.A.*,
589 F.3d 274 (6th Cir. 2009) 38

Motor Vehicle Mfrs. Ass'n v. *State Farm Mut. Auto. Ins. Co.*,
463 U.S. 29 (1983) 21, 31, 38

Nat. Res. Def. Council v. *Nuc. Regul. Comm'n*,
879 F.3d 1202 (D.C. Cir. 2018) 39

Ohio v. *EPA*,
603 U.S. 279 (2024) 21, 24, 28

Pacific Choice Seafood Co. v. *Ross*,
976 F.3d 932 (9th Cir. 2020) 31

Piedra Alvarez v. *Barr*,
829 F. App'x 833 (9th Cir. 2020) 35

Sanders v. *Allison Engine Co., Inc.*,
703 F.3d 930 (6th Cir. 2012) 15

Sofco Erectors, Inc. v. *Trs. of Ohio Operating Engs. Pension Fund*,
15 F.4th 407 (6th Cir. 2021) 12, 19, 21

Tennessee v. *Cardona*,
762 F. Supp. 3d 615 (E.D. Ky. 2025) 11, 12, 32, 33

Third Fed Sav. & Loan Ass'n of Cleveland v. *Fireman's Fund Ins. Co.*,
548 F.2d 166 (6th Cir. 1977) 18

U.S. Sugar Corp. v. *EPA*,
830 F.3d 579 (D.C. Cir. 2016) 39

U.S. Telecom Ass'n v. *FCC*,
359 F.3d 554 (D.C. Cir. 2004) 19

Utility Air Regul. Grp. v. *EPA*,
573 U.S. 302 (2014) 15, 26

W. Va. Univ. Hosps. v. *Casey*,
499 U.S. 83 (1991) 36

Waskul v. *Washtenaw Cnty. Cmty. Mental Health*,
900 F.3d 250 (6th Cir. 2018) 11

West Virginia v. *EPA*,
597 U.S. 697 (2022) 12, 37

Whitman v. *Am. Trucking Ass'ns*,
531 U.S. 457 (2001) 36, 37

Yates v. *United States*,
574 U.S. 528 (2015) 14

Zellmer v. *Meta Platforms*,
104 F.4th 1117 (9th Cir. 2024) 18

Statutes

5 U.S.C. § 706 ..... 11,12, 20

7 U.S.C. § 21 18

12 U.S.C. § 5534 15

12 U.S.C. § 5481 ..... 15, 16

12 U.S.C. § 5511 18

12 U.S.C. § 5512 ..... 18, 20, 37

12 U.S.C. § 5532 14

12 U.S.C. § 5533 ..... *passim*

12 U.S.C. § 5534 15

15 U.S.C. § 78s 18

15 U.S.C. § 1681c-1 36

15 U.S.C. § 1639h 36

15 U.S.C. § 1691 36

15 U.S.C. § 6801 5

Regulations

12 C.F.R. 7.4002 36

12 C.F.R. 30.2 5

12 C.F.R. 364.100 5

12 C.F.R. 1005.6 28

12 C.F.R. 1026.13 29

12 C.F.R. 1033.101 .....7, 8

12 C.F.R. 1033.111 11

12 C.F.R. 1033.121 10

12 C.F.R. 1033.131 .....4, 16

12 C.F.R. 1033.211 .....8, 22, 25

12 C.F.R. 1033.301 .....8, 11, 35

12 C.F.R. 1033.311 .....*passim*

12 C.F.R. 1033.321 .....*passim*

12 C.F.R. 1033.331 .....8, 23

12 C.F.R. 1033.401 7

12 C.F.R. 1033.421 .....7, 8

12 C.F.R. 1033.431 .....7, 17

12 C.F.R. pt. 364, App'x B.....26

Financial Data Exchange, Inc., CFPB No. 2024-CFPB-PFDR-0001 (Jan. 8, 2025) 20, 34

Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74,796 (Oct. 31, 2023) 7, 26, 39

Required Rulemaking on Personal Financial Data Rights; Industry Standard-Setting, 89 Fed. Reg. 49,084 (June 11, 2024) 9, 20, 35

Required Rulemaking on Personal Financial Data Rights, 89 Fed. Reg. 90,838 (Nov. 18, 2024) ..... *passim*

Other Authorities

156 Cong. Rec. E1262-63 (July 1, 2010) 13

114 Million Reasons To Keep Moving Forward on Industry-Led Standard for Secure Data Sharing, Financial Data Exchange (Apr. 25, 2025), https://perma.cc/V75C-E95M 6

American Heritage Dictionary (2022) 16

Board of Governors of the Federal Reserve System, FDIC & OCC, *Interagency Guidance on Third-Party Relationships: Risk Management* (June 6, 2023), https://perma.cc/D55F-26YE 23, 27

CFPB, *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation* (Oct. 18, 2017), https://perma.cc/846R-9GLT 24

Dan Awrey & Joshua Macey, *The Promise & Perils of Open Finance*, 40 Yale J. on Reg. 1 (2023) 22

Restatement (Third) of Agency (2006) 16, 18

Restatement (Third) of Trusts (2003) 16

S. Rep. 111-176 (2010) 13

Webster New World Compact School and Office Dictionary (4th ed. 2002) 13

Webster's Third New International Dictionary (2002) 17

PRELIMINARY STATEMENT

This case involves an agency that drastically overstepped its statutory authority, injected itself into a well-functioning ecosystem that was thriving under private industry initiatives, and installed a burdensome, irrational, and risky regulatory framework in its place. That regime is unlawful many times over. After reviewing the Rule at issue in this case over the past several months, the agency itself agrees that it violates the Administrative Procedure Act. This Court should now enter judgment setting it aside.

The Rule arises out of the recent explosion in new ways that consumers can organize, analyze, and deploy their financial assets. Thanks to rapid technological advances, thousands of companies now offer products or services that involve access to or use of consumers' bank accounts. From budgeting to peer-to-peer payments to stock and cryptocurrency trading, such offerings from these financial technology companies (colloquially known as fintechs) often require consumers to do no more than download an app and allow the fintech to access their account data. This ecosystem has come to be broadly known as "open banking."

Banks welcome the new opportunities to serve their customers that open banking has created. But there are obvious risks. Consumer financial data can be extremely damaging in the wrong hands, especially if it can be used to move money out of consumers' accounts. As a matter of both business necessity and regulatory obligation, banks place the highest priority on protecting their customers' financial information. So to balance that security imperative with the opportunities new technologies bring, banks have worked with other industry actors to develop *secure* open-banking solutions—now serving over a

hundred million accounts and growing—that enable consumers' financial autonomy while protecting their data and assets.

But then the government stepped in. In the Rule challenged here, the Consumer Financial Protection Bureau appointed itself as the czar of open banking in the United States. Ignoring the industry-developed solutions, the Bureau dictated a complex and highly burdensome regime mandating that banks share their customers' sensitive financial data with any third party that can obtain customer authorization. The Rule requires banks to create a dedicated application programming interface (API) meeting highly demanding (yet hopelessly vague) performance standards to facilitate that third-party sharing. And it prohibits banks from limiting third-party access to these APIs, even based on risk concerns, outside of narrowly prescribed circumstances. To top it off, after forcing banks to meet these highly burdensome mandates, the Rule prohibits banks from charging *any* fees to the third-party entities who profit from this data. In short, the Rule gives a windfall to one segment of industry and perversely forces banks to fully subsidize an unworkable regime that will put their customers' data at risk. For several independent reasons—and as the Bureau itself now agrees—the Rule is unlawful and should be set aside.

The first and most fundamental problem is that Congress never authorized the Bureau to do any of this. *See infra* Part I. The Bureau claimed authority for the rule under Section 1033 of the Dodd-Frank Act, which states in relevant part that banks "shall make available to a consumer" certain information about the "financial product or service" the consumer obtains from the bank. 12 U.S.C. § 5533(a). That modest provision—enacted just a few months after the first iPad was announced—did not anoint the Bureau as the

regulator of open banking in the United States. It simply allowed *consumers* to obtain relevant information about the terms and features of their banking products and services.

Having strayed well beyond its authority under Section 1033, the Bureau proceeded to adopt a Rule that is unlawful in several other ways. As another core statutory defect, the Rule impermissibly outsources substantive regulatory choices to private organizations, allowing them to set "consensus standards" that will constitute "indicia" of compliance with the Rule. If Congress authorized the Bureau to set rules for open banking, the Bureau itself must set those rules.

Second, the Bureau's mass consumer data-sharing regime is fundamentally arbitrary and capricious. *See infra* Part II. Taking its various requirements together, the Rule's framework places customers' most sensitive financial data at risk, while simultaneously handcuffing banks in their ability to mitigate that risk and assuming no role for the Bureau itself in policing it. The APA required the Bureau to address and explain the *cumulative* effect of its various policy choices, not simply attempt to justify each individual provision in a vacuum.

Beyond these deficiencies that pervade the entire Rule, several individual provisions are unlawful standing alone. *See infra* Part III. The Rule's requirement that banks share "[i]nformation to initiate payment to or from" the customer's account departs from Section 1033 by requiring banks to enable *functionality* of making payments, when the statute speaks only of providing information about a customer's account. The Rule irrationally restricts banks' ability to refuse to share customer data based on risk concerns, even when required by safety-and-soundness rules enforced by banks' principal financial

regulators. And despite imposing these limits on banks' exercise of their risk-management authority, the Bureau arbitrarily refused to set rules for who should be liable when customers' data is inevitably compromised under its mass data-sharing regime.

The list goes on. The Rule requires the newly mandated APIs to meet demanding performance requirements in processing third-party data requests. But these requirements, most of which depend heavily on "consensus standards" that will be set by private organizations, are so vague and muddled as to leave banks with practically no guidance on how to comply—especially when not a single such "consensus standard" has yet been issued. And despite this vacuum of guidance, the Bureau set fast-approaching, fixed deadlines for banks to come into compliance, rather than dates tied to those forthcoming standards. Finally, in a remarkable act of regulatory overreach, the Rule unlawfully prohibits banks from charging *any* fees to the commercial third parties who directly profit from the Rule's extraordinarily costly mass data-sharing regime.

For all of these reasons, this Court should set aside the Rule.

BACKGROUND

A. Open Banking

The open-banking model allows fintech companies to offer a wide range of financial products and services to bank customers. To provide these services, fintechs need access to a consumer's banking information, including data about transaction history, current balances, and account-identification information. Rather than obtain this information directly from each of their users' banks, fintechs frequently rely on other third parties known as "data aggregators," who make a business out of collecting consumer information, packaging it, and selling it to others. *See* 12 C.F.R. 1033.131.

Banks widely support open banking, so long as their customers' financial data and assets remain protected. *See* AR_916 (Bank Policy Inst. & The Clearing House (BPI & TCH) Cmt. Ltr.) at 1-2; AR_793 (U.S. Bank Cmt. Ltr.) at 1. But security comes first. Congress mandates that each financial institution "protect the security and confidentiality of [its] customers' nonpublic personal information," 15 U.S.C. § 6801(a), and banks' primary regulators implement these and similar directives. *See, e.g.*, 12 C.F.R. 30.2 (acknowledging the Office of the Comptroller of the Currency's responsibility "to establish safety and soundness standards"); *id.* § 364.100 (same for the FDIC).

Striking that balance can be challenging. Millions of consumers seek to participate in some form of open banking, and thousands of fintechs, data aggregators, and other firms now offer such products and services. Those third-party companies generally lack the rigorous data security, consumer-protection controls, and comprehensive regulatory supervision that banks have. Indeed, there have been numerous well-publicized stories of data breaches at fintechs, including due to basic errors. *See* Am. Compl. ¶ 7 & n.2, ECF No. 22. So responsibly addressing consumers' requests to share their bank account data with these third parties can "create difficult challenges for financial institutions." *See* AR_22 (Nov. 17, 2016 remarks of Former Director Cordray).

In addition, some methods third parties use to obtain consumers' financial data are inherently unsafe. That is especially true of "screen scraping," which until relatively recently was the only such method available. Screen scraping involves a third party's use of the consumer's online login information to access the consumer's account and download the associated data. It is particularly dangerous because it routinely leads to third parties'

"scraping" more data than necessary and the indefinite retention of both that data and the customer's login credentials. *See* Required Rulemaking on Personal Financial Data Rights, 89 Fed. Reg. 90,838, 90,840 (Nov. 18, 2024) (Rule or Final Rule).

But recent private initiatives have made significant strides in navigating these risks. Most importantly, APIs have come to replace screen scraping as the preferred method of third-party data access. APIs are software-based protocols that allow two different entities to communicate with each other. An approved third-party company can access a bank's API and retrieve precisely the financial data that the customer and bank have authorized the company to access, updating that information by making additional data requests as often as necessary. *See* AR_877 (Akoya LLC Cmt. Ltr.) at 5; AR_793 (U.S. Bank Cmt. Ltr.) at 1 (reporting "over 1.8 billion API interactions" in 2023). Although information transmission through APIs still carries risks, use of APIs is far superior to screen scraping because it facilitates the secure, targeted sharing of information without the need to obtain (or retain) customers' login credentials.

Banks have actively participated in developing API-based sharing of their customers' data. The Financial Data Exchange, a nonprofit industry-standards body whose members include banks, fintechs, financial data aggregators, and others, has developed an open-banking API specification that is currently used by 114 million consumer accounts.[1] This solution has thrived due to flexible risk-management policies that enable banks to

[1] *114 Million Reasons To Keep Moving Forward on Industry-Led Standard for Secure Data Sharing*, Financial Data Exchange (Apr. 25, 2025), https://perma.cc/V75C-E95M.

facilitate use of open banking while preserving security, including by ensuring banks can decline to share sensitive consumer information with risky third parties.

B. The Bureau's Rulemaking

Despite all this progress in private partnerships, the CFPB decided to arrogate to itself the power to dictate the terms of open banking. The Bureau claimed that Section 1033 of the Dodd-Frank Act authorized it to do so. The relevant language of that provision states that "a covered person"—*i.e.*, a bank—"shall make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person." 12 U.S.C. § 5533(a). From that modest textual hook, the Bureau set out to "address the challenges" it believed to exist in "the open banking system." Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74,796, 74,799 (Oct. 31, 2023) (Proposed Rule).

The Bureau proposed its rule on October 31, 2023. It received over 11,000 comments, many of which criticized fundamental aspects of the Bureau's proposal. Yet the CFPB proceeded to finalize the Rule largely as proposed on October 22, 2024. The Rule's key relevant provisions are summarized below.

Mandatory disclosure to third parties.—The Rule requires banks to share consumer account data with "authorized third parties," including but not limited to fintechs and data aggregators. *See* 12 C.F.R. 1033.101(b). Any entity that obtains the consumer's consent to access the consumer's data and agrees to certain restrictions on use of that data can become an "authorized third party." *See id.* §§ 1033.401, 1033.421. The Rule permits the third party to use a data aggregator to harvest the consumer's data if the data aggregator agrees to be bound by the same restrictions on data use. *Id.* § 1033.431(c). And

the Rule even allows the third party to share data with other parties if it contractually requires them to abide by the Rule's restrictions on data use. *Id.* § 1033.421(f). The third party need not inform the bank or consumer who these other third parties are.

The Bureau plays no gatekeeping role in determining whether a third party may become "authorized" to receive consumer data. Nor does it assume any role in monitoring the third party's compliance with the commitments it makes to obtain authorization. The Rule instead makes *the bank* responsible to "[d]ocument" that "the third party has followed the authorization procedures" before sharing. *Id.* § 1033.331(b)(1)(iii).

Data that must be shared.—The "covered data" that banks must share includes various categories of information about the consumer's account, such as transaction history, account balances, and upcoming bill information. *Id.* § 1033.211(a), (b), (e). Over commenters' objections, *see, e.g.*, AR_882 (JPMC Cmt. Ltr.) at 8-12, covered data also includes "[i]nformation to initiate payment," which "includes"—but is expressly not limited to—an account and routing number that can be used to remove funds from a consumer's account. 12 C.F.R. 1033.211(c).

Mechanism of data sharing.—The Rule requires covered banks to create a new "developer interface," *i.e.*, an API to facilitate the transmission of data to third parties. *See* 12 C.F.R. 1033.301(a), (b)(2); Final Rule at 90,839. The performance of the developer interface must meet various standards set forth in the Rule. As a quantitative matter, it must respond "proper[ly]" to at least 99.5% of requests. 12 C.F.R. 1033.311(c)(1). But even that is not enough to demonstrate an interface's "commercially reasonable" performance. *Id.* §§ 1033.311(c), (c)(1). That standard, under the Rule, also requires assessment of

several qualitative metrics, including the amount of scheduled and unscheduled "downtime," how much notice is given of any such downtime, and how long the interface takes to process requests. *Id.* § 1033.311(c)(2)(ii)(A)-(E). The interface's performance on these metrics is measured based on a nonexclusive three-factor test, which includes a comparison to the performance of the bank's own consumer interface and other banks' developer interfaces, as well as an assessment based on "consensus standards" that will purportedly be issued at some unknown future date. *Id.* § 1033.311(c)(2)(i). And despite commenters' pleas that this interface should fully supplant screen scraping, the Bureau declined to ban that practice. Final Rule at 90,895.

Private standard-setting organizations.—The Rule provides that many standards, including performance requirements for the developer interface, will be set by private standard-setting organizations the Bureau will recognize in the future.[2] These organizations will issue "consensus standards" addressing substantive compliance matters, such as what constitutes "reasonable" (i) "frequency restrictions" on third parties' requests, 12 C.F.R. 1033.311(d); (ii) denials of access based on risk-management concerns, *id.* § 1033.321(c)(1); and (iii) overall interface performance, *id.* § 1033.311(c)(2)(i)(A). An interface's conformance to a consensus standard constitutes "indicia" of compliance with the Rule, which apparently means that meeting such a standard is relevant, but neither necessary nor sufficient to avoid enforcement. *See* Final Rule at 90,862.

[2] The Bureau finalized the portion of its rule regarding how it will recognize standard-setting bodies on June 11, 2024, prior to finalizing the Rule challenged here. *See* Required Rulemaking on Personal Financial Data Rights; Industry Standard-Setting, 89 Fed. Reg. 49,084 (the Standard-Setter Rule).

Risk-management and liability allocation.—The Rule generally mandates that banks share data with all comers and severely constrains banks' ability to deny access based on risk-management concerns. The Rule nominally recognizes that banks may permissibly deny access pursuant to policies to comply with regulatory safety and soundness requirements of their banking regulators, but only if the Bureau *also* deems such denial "reasonable." 12 C.F.R. 1033.321(a). To meet that requirement, the access denial must be "[d]irectly related to a specific risk of which the [bank] is aware" and "[a]pplied in a consistent and non-discriminatory manner." *Id.* § 1033.321(b). The Bureau also declined commenters' request to prescribe rules allocating liability among the various actors when the inevitable misuse or compromise of consumer data occurs. *See* Final Rule at 90,848.

Compliance deadlines.—In response to the Bureau's proposal to set fixed deadlines for compliance, commenters urged that those deadlines should be keyed to standard-setting organizations' unveiling of consensus standards (or, at a minimum, that banks should be given two years to comply with the Rule). *See, e.g.*, AR_882 (JPMC Cmt. Ltr.) at 30-33; AR_879 (Wells Fargo & Co. Cmt. Ltr.) at 12-13. The Bureau nonetheless set fixed deadlines based on a bank's size, starting with 18 months from the announcement of the Rule for the largest banks. 12 C.F.R. 1033.121(b). It did so despite not having recognized a single standard-setting organization (or even indicating when it would) to issue any of the numerous consensus standards that the Bureau made critical to compliance with the Rule.

Prohibition on charging fees.—The Rule indisputably imposes substantial burdens and expense on banks. The Bureau even acknowledged compliance costs of up to $47 million annually. *See* Final Rule at 90,961. But it nonetheless prohibited banks from charging *any*

fees for access to data, even fees limited to recouping costs and charged only to third parties. *See* 12 C.F.R. 1033.301(c).

Small bank exemption.—In one of the few changes from the proposal, the Rule exempts banks with assets of $850 million or less from compliance. *Id.* § 1033.111(d).

C. The Bureau's Concession That The Rule Is Unlawful

Following the change in presidential administration, the Bureau reevaluated the Rule. On February 25 and March 26, 2025, the parties jointly moved to stay proceedings in this litigation for a total of 90 days to allow the Bureau's new leadership to review the Rule. ECF Nos. 40, 42. The Court granted those motions and tolled the Rule's compliance deadlines for an equivalent period. ECF Nos. 41, 45. On May 23, 2025, the Bureau filed a status report advising that it "has determined that the Rule is unlawful and should be set aside," and that it will seek summary judgment to effectuate that result. ECF No. 57.[3]

STANDARD OF REVIEW

"[S]ummary judgment is the appropriate 'mechanism' for adjudicating claims arising under the Administrative Procedure Act." *Tennessee* v. *Cardona*, 762 F. Supp. 3d 615, 622 (E.D. Ky. 2025) (citation and alterations omitted). The APA requires a court to

[3] Plaintiffs undoubtedly have standing to challenge the Rule. Plaintiff Forcht Bank, N.A., is directly regulated by the Rule and will have to expend substantial sums to comply with it. Ex. 1 (Declaration of Forcht Bank, N.A.) at ¶¶ 5-7. Plaintiffs Kentucky Bankers Association and Bank Policy Institute have associational standing: at least one member of each association would have standing to sue in its own right, the interests at stake in this action are germane to each association's purpose and interests, and the relief sought—setting aside the Rule—does not require the participation of individual members. *See Waskul* v. *Washtenaw Cnty. Cmty. Mental Health*, 900 F.3d 250, 254 (6th Cir. 2018); *see also* Ex. 2 (Declaration of Kentucky Bankers Association) at ¶¶ 6, 8-15; Ex. 3 (Declaration of Bank Policy Institute) at ¶¶ 5, 8-11.

"hold unlawful and set aside agency action" that is "in excess of statutory jurisdiction, authority, or limitations." 5 U.S.C. § 706(2)(C). The APA further prescribes that agency action be set aside if it is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." *Id.* § 706(2)(A).

When a rule violates the APA—as this Rule does many times over—"[v]acatur is the normal remedy," due to the APA's directive "that a reviewing court 'shall . . . set aside' unlawful agency actions." *Long Island Power Auth.* v. *FERC*, 27 F.4th 705, 717 (D.C. Cir. 2022) (quoting 5 U.S.C. § 706(2)); *see also Data Mktg. P'ship, LP* v. *U.S. Dep't of Lab.*, 45 F.4th 846, 859 (5th Cir. 2022); *Cardona*, 762 F. Supp. 3d at 627.

ARGUMENT

I. THE RULE EXCEEDS THE BUREAU'S STATUTORY AUTHORITY.

"Agencies have only those powers given to them by Congress." *West Virginia* v. *EPA*, 597 U.S. 697, 723 (2022). The most fundamental problem with the Rule is that Congress has never authorized the CFPB to mandate and regulate open banking. Section 1033 of Dodd-Frank, on which the Rule relies, provides *consumers*, not third parties, with "rights to access information" held by banks. 12 U.S.C. § 5533.

Even if Section 1033 authorized the Bureau to require banks to share consumer data with third parties, the Rule impermissibly outsources much of that authority to private standard-setting organizations. Agencies must at least be able to point to clear congressional authorization to delegate substantive policymaking decisions to private organizations, *Sofco Erectors, Inc.* v. *Trs. of Ohio Operating Engs. Pension Fund*, 15 F.4th 407, 428 (6th Cir. 2021), and the Bureau can point to nothing of the sort in Section 1033.

A. Section 1033 Does Not Authorize The Bureau To Compel Banks To Share Data With Commercial Third Parties (Count I).

As relevant here, Section 1033(a) contains a simple directive: a bank "shall make available to a consumer, upon request, information in the control or possession of [the bank]" that relates to the "consumer financial product or service that the consumer obtained from the [bank]." 12 U.S.C. § 5533(a). The provision received little attention in the lead-up to Dodd-Frank, but was described as simply furthering one of that Act's central goals of "giv[ing] the American people the protections and information they need to be better informed consumers and investors." 156 Cong. Rec. E1262-63 (July 1, 2010) (statement of Rep. Jackson Lee). Section 1033 "ensures that consumers are provided with access to their own financial information," S. Rep. 111-176, at p. 173 (2010), in a "form usable by the consumer," 12 U.S.C. § 5533(a).

In evaluating the Rule's claim that Section 1033 empowers the Bureau to regulate open banking, this Court should "look to the statutory language as 'the starting point for interpretation, and . . . the ending point [as well] if the plain meaning of that language is clear.'" *Davenport* v. *Lockwood, Andrews & Newnam, Inc.*, 854 F.3d 905, 909 (6th Cir. 2017) (internal quotation omitted). The analysis here starts and ends with the term "consumer." Under both that term's plain meaning and other tools of statutory interpretation, Section 1033 does not authorize the Bureau to require banks to share their customers' financial data with commercial third parties.

1. "Consumer" In Section 1033 Means The Individual Consumer.

The ordinary meaning of consumer refers to an individual—"one who buys goods or services for personal needs only rather than to produce other goods." *Consumer*, Webster New World Compact School and Office Dictionary (4th ed. 2002).

The rest of Section 1033 confirms that Congress intended "consumer" to take its ordinary meaning. For one thing, the section is entitled "Consumer rights to access information"—an unlikely repository for sweeping authority to compel banks to share their consumers' information with third-party commercial actors. *See Yates* v. *United States*, 574 U.S. 528, 539-40 (2015) (plurality op.) (statutory section title serves as a "[f]amiliar interpretive guide[]"). And Section 1033 elsewhere uses the word "consumer" in a way that could only refer to the individual customer. For example, the statute refers to information about the "product or service that *the consumer obtained* from" the bank and directs that such information must be "in an electronic form *usable by consumers*." 12 U.S.C. § 5533(a) (emphases added). The statute also cautions that it imposes no duties to "maintain or keep any information about a consumer." *Id.* § 5533(c). None of these provisions makes sense if "consumer" means not just the individual consumer, but any commercial third party the consumer purportedly authorizes. *See Brown* v. *Gardner*, 513 U.S. 115, 118 (1994) (presumption that a word has a consistent meaning in a statute is "surely at its most vigorous when a term is repeated within a given sentence," as in Section 1033(a)).

Section 1033's neighboring provisions further support this reading. Section 1032 requires certain disclosures about a "consumer financial product or service" to "consumers" for the purpose of allowing "consumers to understand" the "costs, benefits, and risks" of those products. 12 U.S.C. § 5532(a). And Section 1034 requires banks to adopt policies for

"provid[ing] a timely response to consumers" in connection with a "complaint or inquiry of the consumer." *Id.* § 5534(a), (a)(1). Again, these provisions, like Section 1033, are naturally read to refer to the individual consumer alone. *See Henson* v. *Santander Consumer USA Inc.*, 582 U.S. 79, 86 (2017) (relying on uses of a term in "neighboring provisions in the Act").

2. The General Definition Of "Consumer" In Section 1002 of Dodd-Frank Does Not Support The Rule.

In the Rule, the Bureau relied on the general definition of "consumer" that Congress provided in Section 1002 of Dodd-Frank for the entire Consumer Financial Protection Act. This definition includes "an agent, trustee, or representative acting on behalf of an individual." 12 U.S.C. § 5481(4); *see* Final Rule at 90,843, 90,863, 90,920-21, 90,930. But even if this Act-wide definition applies—despite strong indications to the contrary—it still would not permit compelled data sharing with "authorized third parties" that are more like sellers or service providers than consumers or their agents.

As an initial matter, there is serious reason to doubt that this general, Act-wide statutory definition expands the ordinary meaning of "consumer" in Section 1033. The Supreme Court has recognized that a term defined on an "Act-wide" basis does not necessarily carry that statutory definition where "statutory context" and "the overall statutory scheme" indicate otherwise. *Utility Air Regul. Grp.* v. *EPA*, 573 U.S. 302, 316-20 (2014); *see Envt'l Def.* v. *Duke Energy Corp.*, 549 U.S. 561, 574 (2007) (presumption that a term takes its "statutory definition" "readily yields" when required by context). The Sixth Circuit has similarly recognized that courts should not reflexively conclude "that a term defined by statute carries the same meaning every time it is used." *Sanders* v. *Allison Engine Co., Inc.*, 703 F.3d 930, 938-39 (6th Cir. 2012) (relying on ordinary meaning of the

word "claim" rather than its statutory definition). Here, as discussed above, all textual and contextual indications suggest that the narrower, ordinary meaning of "consumer" applies in Section 1033, and it would be unnatural to import the general, Act-wide definition wholesale. Even the Bureau acknowledged that the term "consumer" "is commonly used in various consumer finance-related contexts to refer to individuals," Final Rule at 90,863, and principally defined "consumer" that way in the Rule itself. 12 C.F.R. 1033.131.

In any event, the general statutory definition of "consumer" in Section 1002(4) still would not prop up the Rule. Commercial third parties engaged in arm's-length dealings with a consumer are not that consumer's "agent, trustee, or representative acting on [the consumer's] behalf." 12 U.S.C. § 5481(4). Those nouns are legal "terms of art" that are presumed to have their common-law meaning, *Evans* v. *United States*, 504 U.S. 255, 259 (1992), which the Bureau has no authority to redefine, *see generally Loper Bright Enters.* v. *Raimondo*, 603 U.S. 369 (2024). At common law, agents and trustees have a fiduciary relationship that requires an unusual level of trust and confidence and that imposes a duty of loyalty to act for the principal's benefit. *See, e.g.*, Restatement (Third) of Agency § 1.01 (2006); Restatement (Third) of Trusts § 2 (2003). The one-time authorization contemplated by the Rule—perhaps provided when the consumer downloads an app—does not convert the third party into the consumer's agent or trustee. *See* AR_27 (CFPB, Transcript of Symposium) at 9 ("The Clearing House conducted some research . . . that demonstrated that our consumers unfortunately don't understand what they're agreeing to."); AR_203 (Letter from Financial Health Network) at 8 ("Most consumers . . . are not aware of the role that data aggregators play in the process.").

The final term, "representative," takes on a meaning similar to "agent" and "trustee" in Section 1002. *See, e.g.*, *Dubin* v. *United States*, 599 U.S. 110, 124-27 (2023) (interpreting the verb "use" in light of narrower verbs listed alongside it). Accordingly, a "representative" of the consumer under Section 1002 would be "one that represents [the consumer] as agent, deputy, substitute, or delegate [usually] being invested with the authority of the principal." *Representative*, Webster's Third New International Dictionary (2002); *see Representative,* American Heritage Dictionary (2022) ("[a]uthorized to act as an official delegate or agent"). At most, the Section 1002 definition means that persons with a special, fiduciary-like relationship with the "consumer" can exercise the consumer's right to receive information under Section 1033.

Third-party entities establishing arm's-length commercial relationships with consumers do not even resemble agents or fiduciaries. *See* Final Rule at 90,921 (declining to dispute that "authorized third parties" under the Rule are not fiduciaries). The Bureau claimed that the authorization procedures "ensure that third parties . . . are acting on the consumer's behalf," Final Rule at 90,921, but the statutory definition refers to entities acting on behalf of the consumer *in the capacity of agent, trustee, or representative*. "Authorized third parties" under the Rule require no such special relationship. This becomes even clearer given that, as the Rule expressly authorizes, many fintechs use fourth-party data aggregators to retrieve consumers' data. *See* 12 C.F.R. 1033.431. The consumer cannot choose whether the third party uses a data aggregator, or which one. There is no sense in which a fourth-party data aggregator the consumer cannot choose can be deemed as the consumer's "trustee, agent, or representative." And the fact that the

consumer has no say in the third party's use of a data aggregator confirms the third party is not an agent, either. *Third Fed Sav. & Loan Ass'n of Cleveland* v. *Fireman's Fund Ins. Co.*, 548 F.2d 166, 170 (6th Cir. 1977) ("the right to control" the manner in which an agent performs work is a core requirement of an agency relationship); *see* Restatement (Third) of Agency § 8.01, cmt. b (2006) (agent acts "subject to the principal's control").

Under the interpretation of Section 1033 adopted in the Rule, fintechs and data aggregators could be considered "consumers" for purposes of the entire Consumer Financial Protection Act—an interpretation that would make several provisions nonsensical. *See, e.g.*, 12 U.S.C. § 5511(b)(1) (Bureau may ensure "consumers are provided with timely and understandable information to make responsible decisions about financial transactions"); *id.* § 5512(c) (Bureau must "monitor for risks to consumers in the offering or provision of consumer financial products or services," including by considering the "likely risks and costs to consumers associated with buying or using a type of consumer financial product or service"). The Rule offers no justification for that strange result, resorting instead to vague statements that "the substance of the rule aligns with the [Consumer Financial Protection Act] definition of consumer" and "congressional intent." Final Rule at 90,920-21. To the contrary, that interpretation would create unacceptable "dissonance between" the "ordinary meaning" of consumer and "the reach of the [statutory] definition." *Bond* v. *United States*, 572 U.S. 844, 861 (2014). Courts commonly recognize that the ordinary meaning of a defined term can and should inform how to interpret the definition of that term. *See, e.g.*, *id.*; *Zellmer* v. *Meta Platforms*, 104 F.4th 1117, 1124 (9th Cir. 2024) ("The Supreme Court frequently considers the ordinary meaning of a statutorily

defined term.") (collecting cases). Here, the Court should apply that principle to reject an interpretation that would transform third parties more appropriately described as sellers and service providers into "consumers."

B. Section 1033 Does Not Permit The Bureau To Enlist Private Standard-Setting Organizations To Set Compliance Standards (Count VI).

Even if the Bureau has authority to require banks to share customer data with commercial third parties, the Rule is still invalid because it impermissibly outsources that authority to private standard-setting organizations. "Agency subdelegations [of statutory powers] to outside parties are assumed to be improper absent an affirmative showing of congressional authorization." *Sofco Erectors*, 15 F.4th at 428 (citation and quotation marks omitted); *see U.S. Telecom Ass'n* v. *FCC*, 359 F.3d 554, 565-66 (D.C. Cir. 2004). Congress knows how to deputize private organizations to assist agencies, and does so explicitly. *See* 15 U.S.C. § 78s (self-regulatory organizations operating under the SEC, such as FINRA); 7 U.S.C. § 21 (private associations operating under the CFTC, such as the National Futures Association). Silence on the issue, by contrast, reflects "that Congress has not delegated . . . the authority to subdelegate to outside parties." *U.S. Telecom Ass'n*, 359 F.3d at 566.[4]

In justifying its reliance on private organizations, the Bureau cited statutory provisions that empower *the CFPB* (and/or its Director) to set various rules and guidance:

[4] This clear-statement rule is warranted due to the serious constitutional concerns that arise when a private entity exercises regulatory authority. *See, e.g.*, *U.S. Telecom Ass'n*, 359 F.3d at 565; *see also Consumers' Research* v. *FCC*, 109 F.4th 743, 775-76 (5th Cir. 2024) (en banc), *cert. granted*, 2024 WL 4864037 (Mem.) (Nov. 22, 2024). Such concerns should not be present here, as Congress has not authorized the CFPB to delegate its Section 1033(a) authority.

- 12 U.S.C. § 5533(a): Information shall be made available to consumers "[s]ubject to rules *prescribed by the Bureau*" (emphasis added);
- 12 U.S.C. § 5512(b)(1): "The Director may prescribe rules and issue orders *and guidance*, as may be necessary or appropriate to enable *the Bureau* to administer and carry out [its duties]" (emphases added).

See Standard-Setter Rule at 49,086. But these provisions simply confirm it is the *CFPB's* responsibility to prescribe rules and provide guidance to regulated parties.[5]

Nevertheless, in more than a dozen instances, the Rule improperly tasks these private organizations with setting standards of compliance with the Rule's vague substantive requirements. For example, standard-setting organizations will write rules governing when risk-based denials of interface access are permissible. 12 C.F.R. 1033.321(c)(1). They will issue standards addressing allowable "frequency restrictions" on third-party access to the interface, which will require weighing costs to banks against third parties' supposed access rights. *Id.* § 1033.311(d). Private standards will even address the foundational but vague requirement of "commercially reasonable" interface performance. *Id.* §§ 1033.311(c)(2)(i), (c)(2)(i)(A).

Given the Rule's vagueness, banks will have to comply with the "consensus standards" if they hope to avoid an enforcement action. Allowing private organizations to

[5] Unlike these other provisions, 12 U.S.C. § 5533(d) provides that "[t]he Bureau, by rule, shall prescribe standards . . . to promote the development and use of standardized formats for information." Congress's direction that the Bureau issue standards "*to promote the development* and use of standardized formats" arguably authorizes the Bureau to determine that private organizations should develop those "standardized formats." Plaintiffs thus do not challenge the Bureau's decision to look to private organizations to issue standards for technical data formatting issues. *See Financial Data Exchange, Inc.*, CFPB No. 2024-CFPB-PFDR-0001 (Jan. 8, 2025) (approving FDX's application to set standards for data formatting).

set standards guiding an agency's compliance determination is a substantial delegation of regulatory authority because such private standards "lend definite regulatory force to an otherwise broad statutory mandate" and "channel its enforcement." *Ass'n of Am. R.R.* v. *U.S. Dep't of Transp.*, 721 F.3d 666, 670 (D.C. Cir. 2013), *vacated on other grounds*, 575 U.S. 43 (2015). The Bureau cannot delegate this authority to a private organization without express statutory authorization—and it has none here. *Sofco Erectors*, 15 F.4th at 428.

II. THE RULE'S MASS DATA-SHARING FRAMEWORK IS ARBITRARY AND CAPRICIOUS (COUNT II).

Even if the Bureau had authority to require banks to share consumer data with commercial third parties, the overall framework the Bureau adopted is arbitrary and capricious because it failed to justify the cumulative impact of the Rule's provisions on consumer data security. *See* 5 U.S.C. § 706(2)(A).

An agency flunks the APA's reasoned-decisionmaking requirement when it "ignore[s] 'an important aspect of the problem'" it is addressing. *Ohio* v. *EPA*, 603 U.S. 279, 292-94 (2024); *see Motor Vehicle Mfrs. Ass'n* v. *State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43, 52 (1983). "The cumulative effect" of multiple regulatory provisions "is unquestionably an important aspect of the problem," and failing to analyze "the cumulative effect, [or] to explain why it did not," renders an agency's decision arbitrary and capricious. *Alliance for Hippocratic Med.* v. *U.S. Food & Drug Admin.*, 78 F.4th 210, 246 (5th Cir. 2023), *rev'd on other grounds*, 602 U.S. 367 (2024); *see Am. Ass'n of Cosmetology Schools* v. *Devos*, 258 F. Supp. 3d 50, 71 (D.D.C. 2017) ("[T]he [c]ourt looks to the entire regulatory scheme to determine whether an agency acted arbitrarily and capriciously.").

That is precisely the Bureau's failure here. The Rule contains numerous interrelated provisions, and commenters warned not only about the negative consequences of each of those provisions individually, but also about their effects in tandem. *See, e.g.*, AR_882 (JPMC Cmt. Ltr.) at 12-14 (addressing overly demanding rules for risk-management denials together with the Bureau's failure to supervise third parties); *cf.* AR_826 (Cmty. Bankers Ass'n of Ill. Cmt. Ltr.) at 5 (stressing the import of considering the "cumulative effect" of the provisions of the Rule). Responding to comments, the Bureau attempted to explain its various individual choices, but paid little attention to the effect of those choices in combination. The resulting Rule simultaneously (i) increases the risk that consumers' most sensitive data will be compromised while (ii) handcuffing banks in their ability to mitigate that risk to protect their customers. Four key decisions by the Bureau exemplify the arbitrariness of the ultimate framework.

First, the Bureau mandated that banks share information that poses a severe risk of consumer harm. The Rule requires sharing not just information about consumers' transaction histories, monthly bills, and the like, but also "[i]nformation to initiate payment to or from" the account. 12 C.F.R. 1033.211(c). By definition and design, this information enables a third party to remove money from a customer's account. Forced distribution of this information on a scale of millions of consumers creates significantly enhanced risk of compromise of such data, and thus customers' funds. That is why regulators in countries whose legislatures have adopted open-banking regimes have imposed significantly heightened supervision and security requirements as a condition to sharing "payment initiation services." AR_916 (BPI & TCH Cmt. Ltr.) at 12.

Second, the Bureau refused to assume any clear role in ensuring that third parties comply with the Rule. Instead, the Rule deputizes *banks* to police the third parties. Purportedly in response to numerous comments on the proposed rule, the Rule requires banks to "[d]ocument" third parties' compliance with authorization procedures, rather than "confirm" it. 12 C.F.R. 1033.331(b)(1)(iii). But the Bureau immediately went on to erase any meaningful distinction, stating that it "expects data providers generally *will*" actually "confirm authorizations of third parties" before granting access to consumer data. Final Rule at 90,905 (emphasis added). The Bureau's refusal to take any role in vetting third parties stands in stark contrast to countries with established open-banking regimes where any third party seeking access to consumer data must first receive authorization from the government regulator. *See, e.g.*, AR_901 (Teller, Inc. Cmt. Ltr.) at 5; Dan Awrey & Joshua Macey, *The Promise & Perils of Open Finance*, 40 Yale J. on Reg. 1, 15-16 (2023) (citing Open Banking Implementation Entity (OBIE), *Enrolling onto the OBIE Directory: How to Guide* (2021), https://perma.cc/J249-CNFL).

Third, the Rule prohibits banks from denying interface access based on risk concerns, outside of narrow, demanding circumstances that the CFPB will assess for "reasonableness." In particular, such denial must be "[d]irectly related to a specific risk of which the data provider is aware," and "[a]pplied in a consistent and non-discriminatory manner." 12 C.F.R. 1033.321(b). The Bureau claimed—without evidence or reasoning—that "denials made in violation of these procedures carry a significant risk of being pretextual." Final Rule at 90,901. Such narrowly drawn limits on banks' exercise of their core risk-management functions conflict with guidance from federal banking regulators,

who stress the need for flexible risk management in dealing with third parties. *See* Board of Governors of the Federal Reserve System, FDIC & OCC, *Interagency Guidance on Third-Party Relationships: Risk Management*, 15 (June 6, 2023), https://perma.cc/D55F-26YE (*Interagency Guidance on Third-Party Relationships*).

Fourth, the Bureau refused to ban the riskiest method of third-party access to customers' financial data: screen scraping. One of the stated goals of the Rule's mandate that banks create new developer interfaces was to avoid the widely acknowledged risks inherent in screen scraping. Final Rule at 90,922. Yet the Bureau inexplicably rejected commenters' pleas to ban the practice and require use of the developer interfaces the Rule mandates. The Rule allows banks to take steps to block screen scraping, but doing so is costly, complex, and often ineffective because screen scrapers "use sophisticated techniques . . . to deliberately evade [a bank's] security controls." AR_882 (JPMC Cmt. Ltr.) at 4.

The Bureau did not adequately address the combined impact of these decisions. In fact, its few nods to the relationship among these provisions *acknowledged* the risks without justifying that choice. For example, the Bureau admitted that "screen scraping creates data security, fraud, and liability risks . . . particularly because the credentials shared to facilitate data access also typically can be used to move funds [*i.e.*, initiate payments]." Final Rule at 90,972. But "if there is an explanation" for why the Bureau still adopted such a risky regime, "it does not appear in the final rule." *Ohio*, 603 U.S. at 293-94.

III. SEVERAL INDIVIDUAL FEATURES RENDER THE RULE UNLAWFUL.

In addition to the above defects permeating the entire Rule, many aspects of the Rule are unlawful in isolation.

A. Section 1033 Does Not Authorize The Bureau To Require Banks To Share Payment-Initiation Information (Count V).

As described above, the Bureau's decision to require banks to share "[i]nformation to initiate payment to or from" the consumer's account unreasonably increases the risks of the Rule's data-sharing regime by mandating the disclosure of highly damaging information. *See* 12 C.F.R. 1033.211(c). But that requirement is unlawful in its own right because it exceeds whatever statutory authority is conferred by Section 1033.

Section 1033 requires banks to give consumers information *about* their accounts: "information relating to any transactions, series of transactions, or to the account[s] including costs, charges[,] and usage data." 12 U.S.C. § 5533(a). These terms—transactions, costs, charges, and usage data—all refer to descriptive data about an account's activity, features, or characteristics. But the Rule's requirement to share "[i]nformation to initiate payment" is different. 12 C.F.R. 1033.211(c). It mandates sharing a category of information defined by *functionality*—data that can enable payment initiation by third parties, including (but expressly not limited to) account and routing numbers. The distinction is subtle but important: even the Bureau has recognized a core distinction between "[a]uthorized data access" and "payment authorization." CFPB, *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation*, 4 (Oct. 18, 2017), https://perma.cc/846R-9GLT . Section 1033 reflects that same distinction—it speaks about descriptive information, not payment functionality.

The Bureau admitted that it made this category of information "broader" than the other types of descriptive information described in Section 1033, purportedly because it believes that evolutions in payments systems could mean that simple account and routing

numbers may one day be insufficient to initiate payment. Final Rule at 90,872.[6] The Bureau thus defined this category in terms of functionality so that data providers would *always* be required to furnish whatever is necessary to trigger payment initiation. But no reading of Section 1033 suggests that Congress empowered the Bureau to guarantee payment initiation for all time, and "[a]n agency has no power to 'tailor' legislation to bureaucratic policy goals." *Util. Air Regul. Grp.*, 573 U.S. at 325.

B. The Rule's Restrictions On Banks' Core Risk-Management Functions Are Arbitrary And Capricious (Count III).

As discussed above, the Rule significantly restricts banks' ability to deny access to developer interfaces based on risk-management concerns, even pursuant to their core safety and soundness obligations overseen by federal banking regulators. The Bureau did not and could not justify this arbitrary and capricious limitation.

The Proposed Rule would have required that any risk-based denial be "reasonable," which meant "at a minimum" that each denial had to be due to a "specific risk" and "applied in a consistent and non-discriminatory matter." Proposed Rule at 74,871 (proposed 12 C.F.R. 1033.321(b)). Numerous commenters criticized this framework as unduly restrictive, and requested the Rule expressly recognize banks' ability to deny access pursuant to federal banking regulators' safety-and-soundness standards. AR_916 (BPI & TCH Cmt. Ltr.) at 10-11, 52; AR_882 (JPMC Cmt. Ltr.) at 13; AR_914 (Wis. Bankers Ass'n Cmt. Ltr.) at 3. The commenters observed that conflicts between CFPB data-sharing

[6] Fintech-aligned commenters understood that the Bureau's ultimate objective was to encourage risky "pay by bank" transactions, which skyrocketed to 2,348 transactions *per second* in India after the adoption of open banking and government-mandated payment methods there. *See* AR_915 (Plaid Cmt. Ltr.) at 21-22.

standards and federal banking regulators' information-security standards would place banks in an untenable position. *See, e.g.*, AR_916 (BPI & TCH Cmt. Ltr.) at 52.

Somehow, in purportedly responding to these concerns, the Bureau made things worse. The Rule recognizes that a bank may deny interface access pursuant to policies and procedures relating to its safety-and-soundness (and other) obligations—but *only* if the denial is *also* "reasonable" under the Rule. 12 C.F.R. 1033.321(a)(2). To make that additional showing, the bank still must show that the denial is "[d]irectly related to a specific risk of which the data provider is aware" *and* "[a]pplied in a consistent and non-discriminatory manner." *Id.* § 1033.321(b). In other words, banks may deny access based on safety-and-soundness concerns only if such denial is (i) required by safety-and-soundness or other legal policies, (ii) directly related to a specific risk of harm, *and* (iii) consistent with prior denials.

This standard is flawed in many ways, but the most obvious is the conflict it creates with banks' safety-and-soundness obligations. Banks are subject to extensive regulations designed to ensure their safety and soundness. These rules—prescribed and overseen by federal banking regulators such as the Federal Reserve, FDIC, or OCC (but not the CFPB)—are intentionally broad and prophylactic, requiring, for example, banks to prospectively "identify reasonably foreseeable . . . threats that could result in unauthorized disclosure" or misuse "of customer information." 12 C.F.R. pt. 364, App'x B, § III(B)(1). But the Rule's stringent requirements point the opposite direction. They require that any risk-based denial of access be "[d]irectly related to a specific risk of which the data provider is aware" and "[a]pplied in a consistent and non-discriminatory manner." 12 C.F.R.

1033.321(b). And by the Rule's very terms, a bank can deny access based on a risk-management decision driven by safety-and-soundness policies, but still be subject to enforcement by the Bureau. *See* Final Rule at 90,898 ("[S]afety and soundness standards . . . are [a] legal requirement[] that *might* justify denying access.") (emphasis added).

Ensuring that regulated parties have a means to comply with *all* legal obligations is undoubtedly "an important aspect of" any regulatory undertaking, and it is paradigmatically arbitrary and capricious for an agency to ignore conflicts between regulated entities' legal obligations. *Ohio*, 603 U.S. at 293 (citation omitted). Here, the Rule puts banks to an untenable choice: deny access pursuant to safety-and-soundness policies and risk enforcement by the Bureau, or allow access despite such policies and risk enforcement by banking regulators (while putting their customers' data and deposits at risk).

Compounding the problem, the Rule's criteria for "reasonableness" are ill-defined and unduly restrictive on their own terms. The Rule's demand for "consistency" is a poor fit in the rapidly evolving world of open banking, where banks must retain "a flexible, risk-based approach to third-party risk management that can be adjusted to the unique circumstances of each third-party relationship." *Interagency Guidance on Third-Party Relationships*, *supra*, at 15. If a bank determines that it should not have granted access in the past, the Rule would seemingly require the bank to repeat that error or otherwise risk enforcement for being "inconsistent."

The Rule's specificity requirement also unreasonably constrains banks, and is inconsistent with the very nature of risk management. Especially in light of the thousands

of third parties involved, "it would be virtually impossible for data providers to identify specific risks in all cases" where a risk-based denial would be warranted. AR_916 (BPI & TCH Cmt. Ltr.) at 49. Nor is it clear what constitutes a sufficiently "specific" risk to justify denial. And the Bureau's unlawful reliance on standard-setters to set "indicia bearing on . . . reasonableness" only further muddies the picture. *See* 12 C.F.R. 1033.321(c)(1).

C. The Bureau's Refusal To Prescribe Rules Allocating Liability For Data Compromise Is Arbitrary And Capricious (Count IV).

The Bureau likewise failed to justify its decision not to prescribe liability rules for when consumer data is inevitably misused or compromised under its mass data-sharing regime. As the Bureau acknowledged, "commenters, academic researchers, and research institute[s] . . . predicted that the final rule would increase the volume of sensitive financial data accessed by third parties, particularly sensitive information to initiate a payment," which would "increas[e] the risk of unauthorized transactions or other harms." Final Rule at 90,846; *see* AR_916 (BPI & TCH Cmt. Ltr.) at 7, 49, 51-52, 78-79; AR_882 (JPMC Cmt. Ltr.) at 10, 54; AR_949 (CBA Cmt. Ltr.) at 3, 26-27, 48. Existing liability regimes generally hold banks responsible for investigating and compensating for unauthorized transfers. *See* 12 C.F.R. 1005.6, 1026.13. But these frameworks were not designed for the Bureau's mandatory open-banking regime, where massive amounts of data are transmitted to "aggregators and third parties that . . . may not have the same liability or responsibilities [as banks] . . . even where they are at fault." AR_882 (JPMC Cmt. Ltr.) at 9. Because of these dynamics, many commenters urged the Bureau to "mandat[e] a comprehensive approach to assigning liability or safe harbors for [banks]." Final Rule at 90,846-47.

In declining to do so, the Bureau claimed that, because "[a]pplicable payment authorization requirements continue to separately apply," existing liability frameworks under "private network rules, contracts, and other laws" were sufficient to address any increased liability. Final Rule at 90,847. This assertion is wrong. Data aggregators and fintechs have no incentive to bargain for liability allocation when the Rule requires banks to share data for free subject to traditional liability arrangements. *See, e.g.*, AR_949 (CBA Cmt. Ltr.) at 48-50; AR_882 (JPMC Cmt. Ltr.) at 9; AR_916 (BPI & TCH Cmt. Ltr.) at 10, 80. And "other laws" do not fairly allocate liability to the actor responsible for breaches: they largely constrain banks' ability to pursue indemnity and contribution from the parties actually at fault. *See, e.g.*, *Mich. First Credit Union* v. *T-Mobile USA, Inc.*, 108 F.4th 421, 430 (6th Cir. 2024) (holding that financial institutions lack a right of action to seek indemnification under the Electronic Funds Transfer Act, and that the Act simultaneously bars banks from seeking indemnification under state law).

In any case, the Bureau's reasoning as to unauthorized payments dodges the key problem: that in a regime that requires banks to share "information to initiate payment" with *thousands* of unregulated third-party companies with very limited ability to control that sharing, adherence to the "applicable payment authorization requirements" referenced by the Rule is orders of magnitude more costly and complex. Indeed, the Bureau did not dispute that the natural and inevitable consequence of its mass data-sharing regime would be more unauthorized or fraudulent payments. Final Rule at 90,847-48. Neither existing liability principles nor private network rules were designed—or are suited—for the Bureau's mass data-sharing mandate.

The Bureau's reliance on other features of the Rule "to mitigate unauthorized transfer and privacy risks to data providers and consumers" is cold comfort, given that the thrust of the Rule is to require *more* sharing and *reduce* banks' ability to counteract the associated risks. *Id.* at 90,848. Indeed, some of the features the Bureau cites are the plainly inadequate ones addressed above, such as "clarifying that data providers can engage in reasonable risk management activities" and purporting to phase out (but refusing to ban) screen scraping. *Id.* Regardless, the Bureau does not and cannot dispute that substantially more consumer data will be transferred, inevitably resulting in more data compromise.

Finally, the Bureau tried to dodge the issue by claiming that "commenters did not provide legal analysis or factual evidence about the likelihood that data providers would actually incur legal liability" for misuse or mishandling of data by third parties. *Id.* at 90,847-48. But it takes no imagination to see that consumers look first to banks to resolve any compromise of their bank accounts. AR_882 (JPMC Cmt. Ltr.) at 9 (third parties commonly lack customer-service and fraud-investigation capabilities); AR_793 (U.S. Bank Cmt. Ltr.) at 5 (Consumers "rely on their financial institution to address their error resolution claims."). And by narrowly fixating on "legal liability," the Bureau ignores the significant costs banks will incur simply to investigate and remediate data breaches—at a scale of potentially millions of accounts because of the Rule. The fact that commenters could not gin up "factual evidence" of these problems before the Rule takes effect is neither surprising nor problematic. "It is not infrequent that the available data does not settle a regulatory issue," but the agency must still "exercise its judgment in moving from the facts and probabilities on the record to a policy conclusion." *State Farm*, 463 U.S. at 52.

D. The Bureau's Performance Standards For Developer Interfaces Are Unlawfully Vague (Count VII).

The Rule not only requires banks to provide access to developer interfaces, but also mandates that those interfaces meet demanding requirements for performance. But because those performance requirements are as unclear as they are stringent, the Rule ultimately gives banks little idea of what they must do to comply.

An agency acts arbitrarily and capriciously by "'fail[ing] to properly specify' its rules such that [the agency] leaves 'no method by which' a regulated party can 'gauge [its] performance.'" *Pacific Choice Seafood Co.* v. *Ross*, 976 F.3d 932, 945 (9th Cir. 2020) (citation omitted). While an agency may rely on "a 'holistic, multi-factor, weight-of-the-evidence test,'" that test must "define[] and explain[] the criteria the agency is applying." *Firearms Regulatory Accountability Coalition, Inc.* v. *Garland*, 112 F.4th 507, 534 (8th Cir. 2024) (citation omitted). A regulation is impermissibly vague when it leaves "no way of predicting what conduct will violate" it. *Cardona*, 762 F. Supp. 3d at 625.

Here, the Rule threatens a finding of noncompliance if a bank's "developer interface[]" does not perform in a "commercially reasonable" manner. 12 C.F.R. 1033.311(c). But the Rule's extended discussion of what constitutes "commercially reasonable" performance is entirely unclear. The Rule first imposes a (demanding) quantitative metric: a developer interface's performance "cannot be commercially reasonable" if it does not provide a "proper response[]" to at least 99.5% of requests. *Id.* § 1033.311(c)(1). A proper response is defined as one that, among other factors, is delivered "within a commercially reasonable response time." *Id.* § 1033.311(c)(1)(iv)(C).

Meeting that quantitative metric is necessary to demonstrate commercially reasonable performance, but it is not sufficient. The Rule goes on to list five aspects of an interface's performance the Bureau will qualitatively assess: the proper-response rate, the amount of scheduled downtime, the amount of notice of scheduled downtime, the amount of *un*scheduled downtime, and the interface's response time. *Id.* § 1033.311(c)(2)(ii)(A)-(E). These five criteria, in turn, will be evaluated according to three "indicia" of commercially reasonable performance: whether the interface's performance conforms to a consensus standard, how the interface's performance compares to that of other data providers' interfaces, and how the developer interface's performance compares to that of the bank's consumer interface. *Id.* § 1033.311(c)(2)(i)(A)-(C).

With this bewildering set of requirements, factors, and indicia, it is anyone's guess what a bank can do to assure itself that its new interface performs well enough to avoid scrutiny and enforcement by the Bureau. The questions are seemingly endless. To list just a few, what does it mean that a 99.5% proper-response rate is a necessary condition for reasonable performance, but the proper-response rate will also be considered as part of the five more qualitative performance factors? How will those five factors be weighed against each other? How do the three indicia of compliance fit together? Do the requirements shift in the absence of a "consensus standard"? If the Bureau is going to compare one bank's interface performance against others', does that mean that the 50% of interfaces that by definition perform below the median level are all noncompliant?

The ultimate result—perhaps by design—is to leave it entirely to the Bureau's discretion to determine who will be subject to enforcement. Because such a framework

gives banks "no way of predicting what conduct will violate the law," *Cardona*, 762 F. Supp. 3d at 625, it is impermissible under the APA.

E. The Rule's Fixed Compliance Timeline Is Arbitrary And Capricious (Count VIII).

The Bureau's decision to set fixed deadlines for banks to come into compliance with a Rule that (under the Bureau's design) has not even been fully articulated is yet another arbitrary and capricious aspect of the Rule. As discussed at length, the Rule in numerous places purports to define substantive compliance by reference to "consensus standards" set by private organizations. These standards will naturally be afforded great weight by industry participants trying to understand what the Rule requires of them. *Ass'n of Am. R.R.*, 721 F.3d at 672. As commenters pointed out, it therefore makes little sense to require banks to begin spending resources to come into compliance by a date certain before any such standards have been issued. AR_882 (JPMC Cmt. Ltr.) at 31; AR_916 (BPI & TCH Cmt. Ltr.) at 22; AR_949 (CBA Cmt. Ltr.) at 52. That approach will penalize banks who undertake compliance measures earliest, because once standards are announced, they may be forced to incur substantial time and expense to redo their work to conform to those standards. *See* Ex. 1 at ¶ 9; Ex. 2 at ¶ 17; Ex. 3 at ¶ 13; *see also* AR_882 (JPMC Cmt. Ltr.) at 31. Despite these concerns, the Bureau arbitrarily insisted on setting fixed and rapidly approaching compliance dates that are not tied to the issuance of any consensus standards.

The concerns animating commenters' objections are coming to pass. When the Bureau promulgated the Rule, it had not recognized any standard setters. Seven months later, it has recognized only one, and that organization applied only to issue standards concerning technical data formatting issues, not the filling-in of substantive regulatory

mandates. *See Financial Data Exchange, Inc.*, CFPB No. 2024-CFPB-PFDR-0001 (Jan. 8, 2025). Now that the Bureau has conceded that the Rule is unlawful and is seeking its vacatur, there is virtually no prospect that any substantive consensus standards will be issued by anyone in the foreseeable future.

The Bureau acknowledged that "[m]ost commenters" requested "that compliance dates account for the timeline for development of consensus standards." Final Rule at 90,859. And in its preliminary final rule about how it would select standard-setting organizations, the Bureau explained that "waiting to finalize the provisions" governing selection of standard setters would "increase[] costs to industry of complying with any substantive compliance requirements" those organizations set. Standard-Setter Rule at 49,089. Yet the Rule inexplicably prescribes a compliance timeline where the clock is ticking regardless of when standards are set. That decision flouts the Bureau's obligations to reasonably explain its deadlines, *Piedra Alvarez* v. *Barr*, 829 F. App'x 833, 834 (9th Cir. 2020), and to respond to comments that "challenge[d] [the] fundamental premise" of beginning the compliance clock when consensus standards for compliance with substantive requirements do not exist, *MCI WorldCom, Inc.* v. *FCC*, 209 F.3d 760, 765 (D.C. Cir. 2000).

F. The Rule Unlawfully Prohibits Banks From Charging Fees For Access To The Developer Interfaces (Counts IX, X).

Last but certainly not least, after adopting a framework that imposes massive compliance (and liability) costs on banks, *see* Ex. 1 at ¶ 7; Ex. 2 at ¶¶ 10-14; Ex. 3 at ¶¶ 10-11, the Rule bans banks from charging any fees for providing these services to the commercial third parties who profit from the use of this data. 12 C.F.R. 1033.301(c). This prohibition on banks' charging fees to third parties is doubly unlawful. Congress did not

authorize the Bureau to force banks to provide cost-free services to other commercial actors. But even if the Bureau could exercise such power, its decision to adopt a total fee prohibition was arbitrary and capricious.

1. The Access-Fee Prohibition Exceeds The Bureau's Statutory Authority (Count IX).

The Rule's fee prohibition is a striking assertion of regulatory power. It forces banks to expend enormous sums to provide highly efficient and technically complex services to other commercial actors for free. Courts should require clear indications that Congress authorized such burdens on businesses and ordinary free-enterprise principles. *See Whitman* v. *Am. Trucking Ass'ns*, 531 U.S. 457, 468 (2001). The Bureau has none.

Nothing in Section 1033 expressly authorizes the Bureau to decide whether banks may charge fees for providing customer data. That silence is telling: when Congress wants to prohibit private businesses from charging fees, it says so. For instance, the Fair Credit Reporting Act mandates that consumer reporting agencies provide required disclosures "without charge to the consumer." 15 U.S.C. § 1681c-1(a)(2)(B). Even elsewhere in Dodd-Frank, Congress expressly prohibited certain fees: creditors must provide copies of appraisals to certain loan applicants "at no additional cost to the applicant," *id.* § 1691(e)(4), and "without charge" to applicants for high-risk mortgages, *id.* § 1639h(c). The Bureau does not have the authority to implement a fee prohibition in Section 1033 that Congress chose not to include. *See, e.g.*, *W. Va. Univ. Hosps.* v. *Casey*, 499 U.S. 83, 87-88 (1991) (omission of "expert fees" from a provision authorizing recovery of "attorney's fees" rendered expert fees unavailable, given that the same Congress had addressed those categories separately in other statutes).

In the Rule, the Bureau principally relied on the fact that Section 1033 directs banks to make data available to consumers "[s]ubject to rules prescribed by the Bureau." 12 U.S.C. § 5533(a). But that phrase merely allows the Bureau to make rules about the topics addressed in the statutes—such as the specific "information relating to . . . transactions" banks must provide, *id.*, the "formats for [the] information," *id.* § 5533(d), and so on. Nothing in the statute relates to the fees banks may charge.

Without any other foothold in the statutory text, there is no basis to interpret the broad phrase "subject to rules prescribed by" an agency to authorize the agency to decide how much a private business may charge for services. *Cf. Ala. Ass'n of Realtors* v. *Dep't of Health & Human Servs.*, 594 U.S. 758, 764 (2021) (requiring "exceedingly clear language" when Congress "wishes to significantly alter the . . . power of the Government over private property") (citation omitted). The U.S. Code is replete with similar boilerplate grants of rulemaking authority, but such general rulemaking language does not empower numerous agencies to dictate whether and how much businesses may charge for their products and services. *See West Virginia*, 597 U.S. at 723 ("Extraordinary grants of regulatory authority are rarely accomplished through 'modest words,' 'vague terms,' or 'subtle devices.'") (citation omitted).[7]

[7] The same analysis applies to the Bureau's attempt to locate its fee-prohibition authority in its broad mission "to prevent evasion of Federal consumer financial law." Final Rule at 90,884; *see* 12 U.S.C. § 5512(b)(1). Whether banks alone must bear the costs of funding the Bureau's mass data-sharing regime under Section 1033 is a "fundamental detail[]" of the regulatory scheme that Congress did not authorize an agency to address via "vague terms or ancillary provisions." *Whitman*, 531 U.S. at 468.

Inferring broad agency authority to prohibit fees would be especially inappropriate in rules related to banking. "[T]he ability to charge fees" has long been recognized as a "fundamental national bank function." *Monroe Retail, Inc.* v. *RBS Citizens, N.A.*, 589 F.3d 274, 280, 283 (6th Cir. 2009). In fact, the federal banking regulators charged with ensuring banks' safety and soundness *direct* banks to charge fees "according to sound banking judgment and safe and sound banking principles," taking into consideration "[t]he cost incurred by the bank in providing the service." 12 C.F.R. 7.4002(b)(2). Interpreting Section 1033(a) to authorize the Bureau to force banks to provide costly services for free runs squarely into these longstanding principles.

The counterarguments the Bureau set forth in the Rule are unpersuasive. It cited two examples where an agency offered interpretations that banks cannot charge fees for certain services. Final Rule at 90,884 (citing Regulation E comment 11(c)-3; Regulation Z comment 13-2). Those examples implement different statutes, have never been blessed by a court, and by their terms apply only in very narrow and unusual circumstances (*i.e.*, in the event of an actual error involving billing or charges to consumers' accounts). Those interpretations certainly provide no support for the wide recognition of agency authority to ban fees whenever it suits the agency's policy preferences.

2. The Access-Fee Ban Is Arbitrary And Capricious (Count X).

Finally, the fee prohibition is also arbitrary and capricious. The APA requires agencies to "give an explanation when [declining] to adopt less restrictive measures in promulgating . . . rules," *Cincinnati Bell Telephone Co.* v. *FCC*, 69 F.3d 752, 761 (6th Cir. 1995). "[C]onclusory statements" are no substitute for "reasoned explanation as to why the less restrictive alternatives . . . are insufficient." *Id.* (citing *State Farm*, 463 U.S. at 48).

The access-fee ban falls well short of this standard. In the Proposed Rule, the Bureau posited that fees may "obstruct the access right" to data. Proposed Rule at 74,814. Numerous commenters pointed out that the obvious way to address any such "obstruction" was to *limit* fees to some reasonable amount. *See* AR_960 (Am. Bankers Ass'n Cmt. Ltr.) at 11; AR_916 (BPI & TCH Cmt. Ltr.) at 11; AR_881 (Indep. Cmty. Bankers of Am. Cmt. Ltr.) at 7. But the Bureau refused to give meaningful consideration to that obvious alternative, claiming there is no "workable and administrable standard" for what constitutes a "reasonable" fee. Final Rule at 90,886. This "conclusory" dismissal does not satisfy the Bureau's obligation to explain why it rejected this less restrictive alternative. *Cincinnati Bell Telephone Co.*, 69 F.3d at 761.

Notably, the Bureau's sudden professed concern for concrete administrable rules in this context stands in stark contrast to its approach elsewhere in the Rule, where it used broadly worded standards in an apparent effort to reserve maximum enforcement discretion. *See, e.g.*, 12 C.F.R. 1033.311(c) ("A developer interface's performance must be commercially reasonable."); *id.* § 1033.311(d) ("[A] data provider must not unreasonably restrict the frequency with which it receives or responds to requests."). This "unexplained inconsistenc[y]" suggests the access-fee prohibition is less a product of reasoned decisionmaking than a pretext for reaching a predetermined outcome: to shift the costs of the new regime onto banks alone. *U.S. Sugar Corp.* v. *EPA*, 830 F.3d 579, 650 (D.C. Cir. 2016) (collecting cases); *see Nat. Res. Def. Council* v. *Nuc. Regul. Comm'n*, 879 F.3d 1202, 1214 (D.C. Cir. 2018) ("[I]t would be arbitrary and capricious for the agency's decision making to be 'internally inconsistent.'") (citation omitted).

Finally, the Bureau's explanation that the fee prohibition safeguards "the consumer data access right" also rings hollow. Final Rule at 90,886. The Bureau is well aware of the Rule's enormous costs, and it claimed in the Rule that it addressed these concerns in part by exempting from the Rule banks with assets under $850 million. *See id.* at 90,885. But the Rule would be far less costly—perhaps not costly at all—if the Bureau simply allowed *all* banks to pass along their costs as fees to third parties who profit from access to consumer data. Refusing this obvious alternative leaves customers of small banks without vindication of their supposed rights under Section 1033. The Bureau did not and cannot explain why exempting an entire class of financial institutions from the requirements of the Final Rule "better effectuate[s] the consumer data access right described in section 1033" than allowing all banks to recoup their costs through the collection of reasonable access fees charged to third parties. *Id.* at 90,886.

CONCLUSION

For the foregoing reasons, and as Defendants now agree, the Court should grant summary judgment to Plaintiffs and set aside the Rule.

Respectfully submitted,

May 30, 2025

Timothy A. Schenk (KY Bar #92011)
KENTUCKY BANKERS ASSOCIATION
600 W Main Street #400
Louisville, KY 40202
Tel: (502) 582-2453
tschenk@kybanks.com

John Court*
Paige E. Pidano*
BANK POLICY INSTITUTE
1300 I Street NW, Suite 1100 West
Washington, D.C. 20005
Tel: (202) 289-4322
john.court@bpi.com
paige.paridon@bpi.com

* Admitted *pro hac vice*

John T. McGarvey (KY Bar #46230)
MORGAN POTTINGER MCGARVEY
401 South Fourth Street, Suite 1200
Louisville, KY 40202
(502) 560-6759
jtm@mpmfirm.com

/s/ *Judson O. Littleton*
Jeffrey B. Wall*
Judson O. Littleton*
Nathan H. Golden*
SULLIVAN & CROMWELL LLP
1700 New York Avenue, N.W.
Washington, D.C. 20006
Tel: (202) 956-7000
wallj@sullcrom.com
littletonj@sullcrom.com
goldenn@sullcrom.com

Robert A. Flatow*
SULLIVAN & CROMWELL LLP
125 Broad Street
New York, NY 10004
Tel: (212) 558-4000
flatowr@sullcrom.com

Counsel for Plaintiffs Forcht Bank, N.A., Kentucky Bankers Association, and Bank Policy Institute

CERTIFICATE OF SERVICE

I hereby certify that on May 30, 2025, I electronically filed this Brief in Support of Plaintiffs' Motion for Summary Judgment with the Clerk of the Court by using the CM/ECF system, which will send a notice of electronic filing to all counsel of record.

/s/ *Judson O. Littleton*

Counsel for Plaintiffs Forcht Bank, N.A., Kentucky Bankers Association, and Bank Policy Institute