UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF KENTUCKY
LEXINGTON DIVISION

FORCHT BANK, N.A., KENTUCKY BANKERS ASSOCIATION, and BANK POLICY INSTITUTE,

Plaintiffs,

v.

CONSUMER FINANCIAL PROTECTION BUREAU and ROHIT CHOPRA, in his official capacity,

Defendants.

COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

Plaintiffs Forcht Bank, N.A., the Kentucky Bankers Association, and the Bank Policy Institute, by and through undersigned counsel, bring this complaint for declaratory and injunctive relief against Defendants Consumer Financial Protection Bureau and Director Rohit Chopra, in his official capacity, alleging as follows:

INTRODUCTION

1. This is a case about a federal agency overstepping its statutory mandate and injecting itself into a developing, well-functioning ecosystem that is thriving under private initiatives. The rule that Plaintiffs challenge seeks to cut off that private development and replace it with a complicated, expensive, mandatory regulatory framework that Congress never authorized. Worse yet, the framework the agency has adopted is fundamentally unsafe, so the primary result of its overreach will be to harm the very consumers it is charged with protecting.

2. A bank's fundamental mission is to safeguard its customers' deposits while providing services that allow those customers to access and deploy their financial assets in the ways they choose. In recent years, third-party technologies have afforded consumers a number of new ways to access, analyze, and use their financial data, such as their transaction history, account balances, spending trends, and more. While this movement toward "open banking"—a term used to describe the model where consumers authorize third parties to access their financial data in order to provide a finance-related product or service—has provided many benefits to consumers, sharing such sensitive data inherently presents risks to the security of customers' deposits and sensitive financial information.

3. As a common example, a financial-technology (or "fintech") company will offer an app that consolidates and displays in one place a consumer's financial data and assets across various accounts. To provide that service, the fintech company needs to (i) obtain access to data about the consumer's various individual accounts (either directly or through another third-party company known as a "data aggregator"), (ii) make its own copies of the consumer's data, and then (iii) frequently update that information as often as the company deems appropriate (often multiple times a day, even if the consumer is not actively using the service).

4. Initially, such third-party access could occur only through rudimentary methods such as "screen scraping"—*i.e.*, using the customer's login information to access and download account details from online banking portals designed for consumers. But these methods necessarily entail giving those third-party companies access to more data than they need, including the customer's login credentials. This form of data access, as well as the continued storage of the customer's credentials, expose consumers to serious risks of unauthorized access to and misuse of their accounts and sensitive data.

5. To enable consumers to participate in open banking in a safer way, market participants have developed more secure data-sharing practices that "allow[] third-party financial service providers to access consumer banking and financial data via application programming interfaces."[1] Application programing interfaces (APIs) are software-based

[1] Alexey Shliakhouski, *Security in Open Banking: Concerns and Solutions*, Forbes (Aug. 19, 2021), https://www.forbes.com/councils/forbestechcouncil/2021/08/19/security-in-open-banking-concerns-and-solutions.

protocols that allow two different applications to communicate with each other. These interfaces facilitate targeted, safer sharing of information between financial institutions and fintech companies authorized by customers, without sharing login credentials. Over the past three years, secure APIs have displaced screen scraping as the preferred method by which banks participate in open banking.

6. In the United States, the developing open banking system has achieved substantial progress through private-sector efforts. Banks, including Plaintiffs and their members, have embraced this opportunity for innovation because it allows them to develop secure and attractive products for their customers. In other words, open banking is already flourishing through a private, market-based "consumer data sharing ecosystem" in which industry members have been actively participating.

7. But all sharing of consumer data—including through more secure APIs—carries risks. Placing additional copies of consumers' private financial data in the hands of more nonbank third parties necessarily increases the opportunities for that data to be stolen, compromised, or otherwise misused. And those third parties are less regulated than banks, which are subject to extensive oversight and supervision by financial regulators. Indeed, a number of fintech companies have been victimized by data breaches.[2]

[2] *See, e.g.*, Pierluigi Paganini, *Data Leak at Fintech Giant Direct Trading Technologies*, Security Affairs (Jan. 31, 2024), https://securityaffairs.com/158384/security/data-leak-at-fintech-direct-trading-technologies.html; Robert Lemos, *Cyberattack on Fintech Firm Disrupts Derivatives Trading Globally*, Dark Reading (Feb. 2, 2023), https://www.darkreading.com/cyberattacks-data-breaches/cyberattack-fintech-firm-disrupts-derivatives-trading; Olivia Powell, *Revolut Data Breach Exposes Information for More Than 50,000 Customers*, Cyber Security Hub (Sept. 21, 2022),

8. Banks, under the supervision of their prudential regulators, have expertise in managing these kinds of risks. Applying that expertise in this context, industry participants have successfully developed and refined open-banking practices that balance consumers' desire to use the valuable tools fintech companies provide against the foremost priority of protecting consumers' deposits and private data. As a result, open banking is flourishing through a private, market-based "consumer data sharing ecosystem" in which industry members have been actively participating. Bank Policy Institute & The Clearing House, Comment Letter on Rule, Docket No. CFPB-2023-0052, at 45 (Dec. 29, 2023), https://www.regulations.gov/comment/CFPB-2023-0052-0918 (BPI & TCH Cmt. Ltr.).

9. That all changed when the CFPB stepped in to announce its new open-banking regulatory regime. Claiming the authority of a provision of the Dodd-Frank Act enacted more than fourteen years ago, the Bureau now seeks to jettison the developing, industry-driven system and replace it with a complicated, costly, and fundamentally insecure mandatory data-sharing framework. *See* CFPB, *Required Rulemaking on Personal Financial Data Rights*, (Oct. 22, 2024), https://www.consumerfinance.gov/rules-policy/final-rules/required-rulemaking-on-personal-financial-data-rights/ (to be codified at 12 C.F.R. part 1033) (the Rule or Final Rule). Rather than increasing consumers' ability to securely access and share their data, the Rule will impede banks' ability to protect consumers, stifle growth and innovation in open banking, and increase risks to consumers'

---

https://www.cshub.com/attacks/news/revolut-data-breach-exposes-information-for-more-than-50000-customers.

deposits and data. Simply put, forcing banks to liberally share customers' sensitive financial information while handcuffing banks from managing the risks of doing so is a recipe for fraud and misuse of customer data.

10. In its proposed rule, published October 31, 2023, the Bureau proposed to install for the first time a federal regulatory regime governing "open banking"—a term or concept that appears nowhere in the governing statute. Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74,796 (Oct. 31, 2023), https://www.govinfo.gov/content/pkg/FR-2023-10-31/pdf/2023-23576.pdf (Proposed Rule). Among other things, the Bureau proposed to (i) mandate the sharing of sensitive customer data such as transaction history, account balances, and even account and routing numbers through APIs with a seemingly unlimited number of third parties; (ii) force banks to oversee and be responsible for those third parties' security practices, while simultaneously limiting banks' authority to stop sharing based on risk-management concerns; (iii) outsource authority to private "standard setters" to set the rules of regulatory compliance; (iv) set entirely unrealistic deadlines to come into compliance with the new rule; and (v) prohibit banks from collecting any fees from third parties in exchange for the newly mandated service.

11. Given these deeply problematic aspects of the proposal, the Bureau heard from more than 11,000 commenters, many of whom requested substantial changes. *See, e.g.*, BPI & TCH Cmt. Ltr., *supra* ¶ 8; JPMorgan Chase & Co., Comment Letter on Rule, Docket No. CFPB-2023-0052 (Jan. 2, 2024), https://www.regulations.gov/comment/CFPB-

2023-0052-0975 (JPMC Cmt. Ltr.). The Bureau nonetheless finalized its rule largely as proposed on October 22, 2024, retaining nearly all the problematic features of its proposal.

12. The Bureau's bureaucratic intervention into a well-functioning area that is rapidly developing and improving through private initiatives is not just unnecessary; it is counterproductive, and it will ultimately harm consumers, the very group the Bureau is charged with protecting. For a number of reasons, it is also unlawful.

13. *First* and most fundamentally, the Bureau exceeded its statutory authority by requiring banks to broadly provide their customers' financial information to purportedly "authorized" third parties like fintech companies and data aggregators. The Bureau issued the Rule pursuant to Section 1033 of the Dodd-Frank Act, which requires banks to "make available *to a consumer*, upon request, information in the control or possession of the [bank] concerning the consumer financial product or service that *the consumer obtained*" from the bank. 12 U.S.C. § 5533(a) (emphases added). That provision—sandwiched between a provision requiring periodic affirmative disclosures "*to consumers*" about the risks and benefits of their financial products, 12 U.S.C. § 5532(a) (emphasis added), and a provision concerning banks' and regulators' timely "response *to consumers*" regarding "complaints" or "inquiries," 12 U.S.C. § 5534(a) (emphasis added)—requires banks to give *consumers* their *own* information. And although the Act generally defines "consumer" to include "an agent, trustee, or representative acting on behalf of an individual," 12 U.S.C. § 5481(4), the Rule requires data providers to share consumer information with thousands of commercial entities that plainly do not qualify as agents, trustees, or representatives of those consumers. In short, nothing in Section 1033 authorizes the Bureau to dictate terms on

which banks must furnish consumers' data to innumerable, as-yet-unidentified *third parties*—with unknown credentials or security protocols—that are far less regulated than banks, pose potentially novel risks, and have no special relationship with the consumer who requests the data.

14. *Second*, the Bureau inexplicably designed the Rule in a way that substantially increases security risks to consumers while refusing to increase—or even reducing—the level of security protection that will be afforded to those customers' deposits and data. On the risk side, the Bureau decided to require banks to provide access not only to information about a customer's account, but also to information enabling third parties to *initiate payment from that account*. On the security side, having ordered banks to provide this sensitive data to third parties, the Bureau declines to assume the primary responsibility for ensuring those third parties can be trusted with that data. Instead, the Rule:

- imposes upon *banks* a vague duty to "document" the compliance with consumer authorization requirements of potentially thousands of fintechs and data aggregators, which are not subject to the same data security requirements and expectations as banks, *see* Final Rule at 576 (to be codified at 12 C.F.R. 1033.331(b)(iii));
- substantially limits banks' ability to deny access to those third parties on risk-management grounds by purporting to confine that discretion to narrowly prescribed circumstances, *see* Final Rule at 574 (to be codified at 12 C.F.R. 1033.321);

- declines to require the third-party fintech companies and data aggregators to use the APIs that the banks will be forced to build, thus permitting the continued use of the screen-scraping method of obtaining consumer data that even the Bureau admits is a serious security risk; and
- refuses to articulate any principles for allocating liability among the various actors in this transmission chain when consumer data is misused, compromised, or stolen.

The Bureau failed to persuasively justify why it rejected comments pointing out these issues (and in fact made some of them even worse in the final rule). The end result is a regime that, in addition to being outside the Bureau's statutory authority, is quintessentially arbitrary and capricious.

15. *Third*, in addition to tasking banks with the obligation to "document" third-party security practices and regulatory compliance, the Bureau outsourced the authority to set standards for compliance to private, third-party organizations. In several key respects, the Rule provides that banks' compliance with the obligation to share information will be measured by compliance with standards set by private standard setters. But nothing in Section 1033 or any other statutory provision authorizes the Bureau to let private organizations decide policy or legal questions that determine banks' compliance with regulatory mandates. The Bureau explained that technical specifications for APIs may become obsolete more quickly than the Bureau can act. *See* Proposed Rule at 74,801. But reference to private standard setters for technical formatting requirements is a far cry from relying on standard setters for policy and legal questions regarding banks' risk-

management practices and reasonable limitations on interface access. This kind of delegation of regulatory authority to a private organization raises serious constitutional questions, but is in any event unauthorized by the statute.

16. *Fourth*, the Bureau imposed a timeline for data providers to come into compliance with the Rule that is fundamentally incompatible with its dependence on standard setters to determine rules for compliance. As explained, the Bureau will depend heavily on private standard-setting organizations to give particularized content to many more general provisions of the rule. But no such "consensus standards" exist today; indeed, the Bureau has not even recognized a single standard-setting organization. The Bureau's decision to set compliance deadlines on dates certain, without regard to when any such standard setter issues any such "consensus standard," is arbitrary and irrational because it starts a clock for compliance with entirely unknown standards.

17. *Fifth and finally*, having imposed these enormous out-of-pocket costs and exposed banks to a substantial and unreasonable risk of liability, the Rule impermissibly bans banks from charging *any* fees designed to recoup those costs to the third-party fintechs and aggregators who will profit from the new framework. Section 1033 does not authorize the Bureau to adopt such a one-sided fee prohibition that effectively gives a windfall to commercial entities like fintechs and data aggregators.

18. For all these reasons and as explained below, this Court should bring a halt to the Bureau's unlawful efforts to force banks to engage in unsafe dissemination of their customers' personal financial information and set aside the Rule under the Administrative Procedure Act (APA).

PARTIES

19. Plaintiff Forcht Bank, N.A. (Forcht Bank), is a federally chartered, community-focused bank that has been serving Kentuckians since 1985 and has its principal place of business at 390 W. Main Street, Lexington, Kentucky. Forcht Bank has over $1 billion in total assets.

20. Plaintiff Kentucky Bankers Association (KBA) is a Kentucky non-stock, nonprofit corporation created pursuant to Kentucky Revised Statutes 273.161 through 273.369 that has its offices at 600 W. Main Street, Suite 400, Louisville, Kentucky 40202. KBA is a trade association that has as members approximately 150 national banks, state banks, and savings banks representing virtually all the commercial banking industry in Kentucky. KBA has been in existence since 1891, and it was formally incorporated in its present form in 1911. According to Article III of the KBA's Articles of Incorporation, the "purposes of the Association are to promote the general welfare and usefulness of banks, trust and title companies, and financial institutions doing business in the Commonwealth of Kentucky; to cultivate a more intimate social and business relation between the representatives of such institutions; to collect and disseminate financial and economic information; to secure unity of action." KBA has members who reside and/or operate in the Eastern District of Kentucky, have at least $850 million in total assets, and will be adversely affected by the Rule. KBA also has members with at least $250 billion in total assets and therefore are subject to the Rule's shortest compliance deadline. *See* Final Rule at 561 (to be codified at 12 C.F.R. 1033.121(b)(1))

21. To further its core purposes of advocating for the financial-services industry, the KBA has challenged numerous rulemakings and other actions of federal agencies, including the Bureau. *See, e.g.*, *Monticello Banking Co.* v. *CFPB*, No. 6:23-cv-148-KKC (E.D. Ky. filed Aug. 11, 2023).

22. Plaintiff Bank Policy Institute (BPI) is a nonpartisan public policy, research, and advocacy group that represents universal banks, regional banks, and the major foreign banks doing business in the United States. BPI produces academic research and analysis on regulatory and monetary policy topics, analyzes and comments on proposed regulations, and represents the financial-services industry with respect to cybersecurity, fraud, and other information-security issues. A 501(c)(6) nonprofit headquartered in Washington, D.C., BPI has members who operate in the Eastern District of Kentucky, have at least $850 million in total assets, and will be adversely affected by the Rule. BPI also has members with at least $250 billion in total assets and therefore are subject to the Rule's shortest compliance deadline. *See* Final Rule at 561 (to be codified at 12 C.F.R. 1033.121(b)(1)).

23. To further its core purpose of advocating for the financial-services industry, BPI has frequently submitted comments on proposed agency rules and participated in litigation concerning regulations of banks. *See, e.g.*, BPI & TCH Cmt. Ltr., *supra* ¶ 8; Bank Policy Institute, Comment Letter on Proposed Agency Information Collection Activities (Mar. 26, 2024), https://bpi.com/wp-content/uploads/2024/03/BPI-Call-Report-FFIEC-101-and-FFIEC-102-Revisions-Comment-Letter-3.26.24-.pdf; Br. for BPI & TCH as *Amici Curiae*, *Custodia Bank* v. *Fed. Res. Bd. of Govs.*, No. 24-8024 (10th Cir. Sept. 4, 2024); Br.

for BPI as *Amicus Curiae*, *McShannock* v. *JPMorgan Chase Bank, N.A.*, No. 19-80030 (9th Cir. Mar. 15, 2019).

24. KBA and BPI bring this action on behalf of their members to advance their members' interests as well as the interests of the entire financial-services community. As part of advocating for their members, these association Plaintiffs are committed to ensuring safe banking practices and a stable and predictable regulatory environment that allows banks to protect their customers and manage their own liability.

25. The Rule imposes direct, burdensome obligations on the association Plaintiffs' members. Accordingly, BPI and its members submitted comments opposing many features of the Rule. *See, e.g.*, BPI & TCH Cmt. Ltr., *supra* ¶ 8; JPMC Cmt. Ltr., *supra* ¶ 11; Wells Fargo & Company, Comment Letter on Rule, Docket No. CFPB-2023-0052 (Dec. 29, 2023), https://www.regulations.gov/comment/CFPB-2023-0052-0881.

26. Defendant Consumer Financial Protection Bureau is a U.S. governmental agency headquartered in Washington, D.C. The Commission is subject to the APA pursuant to 5 U.S.C. § 551(1).

27. Defendant Rohit Chopra is the Director of the Bureau. He is sued in his official capacity and is also subject to the APA pursuant to 5 U.S.C. § 551(1).

JURISDICTION AND VENUE

28. Plaintiffs bring this action under the APA, 5 U.S.C. § 551 *et seq*. This Court has jurisdiction pursuant to 28 U.S.C. § 1331 because Plaintiffs' claims arise under the Constitution of the United States and the APA. The Court has the authority to grant the

requested declaratory and injunctive relief under the APA, 5 U.S.C. §§ 702-706, and the Declaratory Judgment Act, 28 U.S.C. §§ 2201-2202.

29. Forcht Bank has standing because it is directly and adversely affected by the Rule's requirement to develop interfaces for third party access to their consumers' data, including the substantial compliance costs imposed by the Rule and the prohibition on charging any fees to third parties or aggregators to recoup those costs. Forcht Bank is also adversely affected by the increased risk of liability it faces because the Rule does not permit it to take adequate steps to safeguard the security of its customers' financial information or protect it from liability in the event of misuse.

30. KBA and BPI each have associational standing to bring this suit on behalf of, and to seek judicial relief for, their respective members. Their members are directly and adversely affected by the Rule and accordingly have standing to sue in their own right. Specifically, Plaintiffs' members will be harmed by the Rule's requirement to build an expensive interface for disseminating consumers' information; by the unpredictable framework the Rule prescribes, which is heavily dependent on external standard setters who lack regulatory authority (as well as democratic accountability); by uncertain liability regimes that are likely to leave Plaintiffs' members facing significant legal costs because of the Rule's compelled dissemination of information to non-consumer third parties; and by the inability to charge fees for the services the Rule compels them to provide—even fees charged to commercial fintech companies or data aggregators that profit from use of the data. Finally, neither the claims asserted nor the declaratory and injunctive relief requested requires an individual member to participate in the suit. *See Association of Am.*

Physicians & Surgeons, Inc. v. *U.S. Food & Drug Admin.*, 13 F.4th 531, 537 (6th Cir. 2021) (citing *Hunt* v. *Wash. State Apple Advert. Comm'n*, 432 U.S. 333, 343 (1977)).

31. Venue is proper in this district pursuant to 28 U.S.C. § 1391(e) because it is an action against an agency and officer of the United States, no real property is involved, and Plaintiff Forcht Bank resides in this district. Venue is proper in this division because Plaintiff Forcht Bank resides in this division.

BACKGROUND

A. Open Banking

32. Open banking generally refers to a model of structuring the financial-services industry in which a bank customer's financial data, with the customer's permission, can be easily shared with other companies, including other financial-services providers.

33. An explosion in the number of fintech companies offering various finance-related services to consumers has driven the expansion of the open-banking system. Visa reports that 87% of Americans use some sort of open-banking service.[3] For example, a fintech company might offer a product that aggregates all of a consumer's information and assets across all their accounts so the accounts and information may be viewed in one place. Another type of fintech company includes payment-processing applications that allow for

[3] Visa, *What Is Open Banking?* (Jan. 27, 2023), https://usa.visa.com/visa-everywhere/blog/bdp/2023/01/27/what-is-open-1674845638965.html; *see* J.P. Pressley, *Open Banking and APIs: What IT Leaders Need To Know*, BizTech Magazine (Apr. 30, 2024), https://biztechmagazine.com/article/2024/04/open-banking-and-apis-what-it-leaders-need-know-perfcon ("Have you used CashApp or Venmo to pay friends back for picking up a dinner check? That's open banking.").

transferring funds held at banks among individuals.[4] Still other fintech companies serve more specialized functions, such as applications designed for those who are self-employed, or for landlords, or for other categories of consumers or market participants who face common financial issues.

34. Rather than individually communicate with every financial institution fintech companies' customers use, these companies will often delegate data collection to data aggregators to assist them in compiling and updating consumers' account information. Data aggregators—as the name implies—are companies that aggregate a particular dataset from various sources. In the open-banking context, the Bureau defines data aggregators as "person[s] that [are] retained by and provide[] services" to a company "to enable access to covered [consumer] data." Final Rule at 564 (to be codified at 12 C.F.R. 1033.131). Such persons include business "entities." *Id.* at 102.

35. In recent years, industry-led developments have improved the security of open banking practices. Initially, sharing customers' financial information occurred through screen scraping, an insecure process of sharing financial data whereby a third party obtains access to the consumer's login credentials in order to "scrap[e]" that user's "account data." Han-Wei Liu, *Two Decades of Laws and Practice Around Screen Scraping in the Common Law World and Its Open Banking Watershed Moment*, 30 Wash. Int'l L.J. 28, 30 (2020). But when screen scraping is used, the consumer generally has no knowledge

[4] *See* Marielle Segarra, *You May Already Be Using "Open Banking." What Exactly Is It?*, Marketplace (June 24, 2021), https://www.marketplace.org/2021/06/24/you-may-already-be-using-open-banking-what-exactly-is-it.

or control over what and how much data is actually being "scraped," or how frequently. In addition, screen scraping presents excessive risks to the consumer. Third parties often retain the login credentials and (potentially all) account information indefinitely—rendering it vulnerable to being stolen or misused—and/or scrape "more information than is necessary to provide the beneficial service the customer wants."[5] For these reasons, many banks have resisted or actively blocked screen scraping.[6]

36. Increasingly, the industry is transitioning to more secure and targeted sharing of customers' data through APIs. An API operates like a set of instructions by which a third party, pursuant to consumer directive, requests certain specified information from the customer's bank account, and the bank responds to that request with the appropriate information. This method removes any need for the customer to share (or the third party to use or retain) the customer's login credentials. And because APIs allow the consumer and the bank to control what data is shared in response to requests controlled and verified by the consumer, they allow for the targeted transmission of data consumers want to be shared without allowing the indiscriminate "scraping" of data from an online banking portal.

---

[5] *Fidelity Takes Steps to Address Screen Scraping,* Fidelity (Sept. 18, 2023), https://newsroom.fidelity.com/pressreleases/fidelity-takes-steps-to-address-screen-scraping/s/2f33bc18-f16d-4b66-9868-626ada9ba32b.

[6] *See, e.g.*, *id.*; Robin Sidel, *Big Banks Lock Horns with Personal-Finance Web Portals*, Wall St. J. (Nov. 4, 2015), https://www.wsj.com/articles/big-banks-lockhorns-with-personal-finance-web-portals1446683450; *see also* Proposed Rule at 74,797 (referring to the "inherent risks" of screen scraping, "such as the proliferation of shared consumer credentials and overcollection of data").

37. Banks have been active participants in developing API-based open banking through private-sector initiatives. The Financial Data Exchange, a nonprofit industry standards body whose members include financial institutions, fintech companies, financial data aggregators, and others, has developed an open-banking API specification that is being used by 94 million consumer accounts.[7]

B. Information-Sharing Risks

38. Data is only as secure as the weakest link in the chain of transmission. As open banking has facilitated more widespread transmission of consumer data, hackers and other bad actors have more targets to choose from in attempting to access that data for illicit or other improper purposes. Unsurprisingly, they have been trying (and at times succeeding), *see* Paganini, *supra*, note 2; Lemos, *supra*, note 2; Powell, *supra*, note 2.

39. One reason that sharing customer data increases risks is because fintech companies and data aggregators are subject to far less robust requirements and significantly less oversight and supervision than traditional financial institutions. Statement of Donna Murphy, Deputy Comptroller, OCC, Before the Subcommittee on Digital Assets, Financial Technology and Inclusion Committee on Financial Services, U.S. House of Representatives, 4–5 (Dec. 5, 2023) https://www.occ.gov/news-issuances/congressional-testimony/2023/ct-occ-2023-133-written.pdf, (referring to risks

[7] *FDX Hits 94 Million Accounts, CFPB Publishes FDX's Standard-Setting Application*, Financial Data Exchange (Sept. 26, 2024), https://financialdataexchange.org/FDX/News/Announcements/FDX%20Hits%2094%20Million%20Accounts,%20CFPB%20Publishes%20FDX's%20Standard-Setting%20Application.aspx.

posed by "non-bank fintech companies"). Such companies also have less experience in safeguarding information, which can lead to basic mistakes.[8] And of course, once data has left the hands of the bank, it is no longer subject to the bank's monitoring and compliance requirements, or its fraud detection systems.

40. These third parties also have fundamentally different business models and incentives as compared to banks. Banks' principal mission is to ensure their customers can securely deposit, access, and use their funds to further their financial goals. Fintech companies, in contrast, may offer services to customers in exchange for targeted advertising or referral fees for other services.[9] Data aggregators, for their part, are literally in the business of collecting and selling as much customer data as possible.[10]

---

[8] *See, e.g.*, Felix Hacquebord et al., *Ready or Not for PSD2: The Risks of Open Banking*, Trend Micro Research 11 (2019), https://documents.trendmicro.com/assets/white_papers/wp-PSD2-The-Risks-of-Open-Banking.pdf (describing a fintech company that allowed its customers' "email address[es], password[s], [and] client secret authentication[s] [to be] visible in the path of the [f]in[t]ech's API URL"—as in, in the website address for their API).

[9] *See, e.g.*, Tom Sullivan, *How Does Fintech Make Money? 9 Business Models Explained*, Plaid (Oct. 3, 2022), https://plaid.com/resources/fintech/how-does-fintech-and-plaid-make-money/.

[10] *See generally,* Julian Alcazar & Fumiko Hayashi, *Data Aggregators: The Connective Tissue of Open Banking*, Federal Reserve Bank of Kansas City (Aug. 24, 2022), https://www.kansascityfed.org/Payments%20Systems%20Research%20Briefings/documents/9012/PaymentsSystemResearchBriefing22AlcazarHayashi0824.pdf; Karl Popp, *Revenue Models for Aggregator Companies*, Dr. Karl Michael Popp (May 6, 2024), https://www.drkarlpopp.com/karl-michael-popps-blog/revenue-models-for-aggregator-companies.

41. Customers can suffer serious consequences when their financial data is compromised while in the possession of commercial third parties that lack the extensive security practices (and regulatory supervision) that banks have.

42. For instance, consider the widespread fraudulent technique of social engineering.[11] Many consumers may be accustomed to ignoring random text messages inquiring about a recent $100 purchase at a retailer that they know they did not make. But if the bad actor sending the text message has obtained the consumer's transaction history, the bad actor may be able to refer instead to an actual transaction the consumer did undertake, thereby increasing the risk that the customer will believe the text is credible and comply with the bad actor's requests.

43. Compromises of other kinds of consumer financial data can lead to even more direct consequences. A bad actor that gains access to certain information required to initiate payment from a bank account—such as the routing and account numbers—may be able to trigger payments from the account without interacting with the customer at all.

44. These consequences frequently are borne by vulnerable persons. The FBI reported that fraud-related losses by those age 60 and over increased 11% in 2023, to $3.4 billion total. *Elder Fraud, In Focus,* FBI (Apr. 30, 2024), https://www.fbi.gov/news/stories/elder-fraud-in-focus. Many of those losses result from

[11] *See* IBM, *What Is Social Engineering?* (accessed Oct. 17, 2024), https://www.ibm.com/topics/social-engineering.

technology-related scams—such as those related to cryptocurrency, offers of tech support, and personal data breaches. *Id.*

45. Before the Rule at issue here, banks had been managing the risks related to open banking consistently with their commitment to protecting their customers and the guidance of their prudential regulators. More broadly, those regulators have recognized the obvious fact that sharing customer financial information with third parties poses risks. In recent interagency guidance addressing third parties that banks *choose* to form a contractual relationship with, the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency warned banks that "the use of third parties, especially those using new technologies, may present elevated risks to banking organizations and their customers." *Interagency Guidance on Third-Party Relationships: Risk Management* 4 (June 6, 2023), https://occ.gov/news-issuances/news-releases/2023/nr-ia-2023-53a.pdf; *see id.* at 13 (reporting that a number of commenters on the proposed guidance "discussed . . . relationships with fintech companies" and "data aggregators" as examples of third-party relationships that "may pose heightened or novel risk management considerations"). The appropriate way to manage those risks, the banking agencies advised, is for banks to implement "a flexible, risk-based approach to third-party risk management that can be adjusted to the unique circumstances of each third-party relationship." *Id.* at 15.

46. These risks are even more substantial in the context of open banking, where banks must decide whether and how to share consumers' personal and financial information with potentially thousands more third parties with which banks have no voluntary, ongoing

relationship. As Acting Comptroller of the Currency Michael Hsu cautioned in a recent speech about open banking, "[s]ecurity is a prerequisite for the sharing and receiving of consumer financial data," and the "increase in the volume and complexity of consumer-permissioned sharing" brought about by open banking "may introduce new risks and necessitate new controls." Michael J. Hsu, Remarks at FDX Global Summit: "Open Banking and the OCC," at 4 (Apr. 19, 2023), https://www.occ.gov/news-issuances/speeches/2023/pub-speech-2023-38.pdf.

47. Bank regulators outside the United States also have long recognized the risks associated with open banking, especially when it involves payment initiation. European regulators have had a regulatory framework governing open banking in place since 2015. Although those jurisdictions' regulatory frameworks have their own serious flaws, they have notably carved out an active role for regulators in ensuring the safety and security of open banking. For example, in the United Kingdom, any third party seeking to access consumers' financial data must receive authorization to do so from the Financial Conduct Authority, which then monitors the third parties' compliance with applicable regulations. *See, e.g.*, 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).

48. Also relevant here, regulators in both the European Union and the United Kingdom recognize that certain consumer financial data is so sensitive that it warrants extra protection. Specifically, they draw a distinction between "account information services" and "payment initiation services"—the latter of which involves the sharing of

information sufficient to remove money from an account (such as an account and routing number)—and require significantly heightened supervision, liability, and security for payment initiation services. *See* BPI & TCH Cmt. Ltr., *supra* ¶ 8, at 12.

49. In the Rule at issue in this case, the CFPB has sought to install a regulatory framework governing open banking for the first time in the United States. The most fundamental problem is that Congress did not authorize the Bureau to do so. But on top of that, the Bureau inexplicably adopted an approach that—contrary to federal banking regulators' guidance and in stark contrast to other open-banking regimes—puts customers' most sensitive information at risk, yet abdicates the Bureau's responsibility to mitigate that substantially increased risk. The end result is a framework that threatens significant harm to consumers and the entire financial-services ecosystem.

THE BUREAU'S RULEMAKING

50. The rule at issue in this case purports to be the rulemaking required under Section 1033 of the Dodd-Frank Act. The CFPB proposed the rule on October 31, 2023, thirteen years after Dodd-Frank was passed. Having neglected its obligation to issue a rule under Section 1033 for thirteen years, the CFPB appears to have sought to mask that inaction by proposing a rule going far beyond Section 1033. Section 1033(a) states:

> Subject to rules prescribed by the Bureau, a covered person 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, including information relating to any transaction, series of transactions, or to the

> account including costs, charges and usage data. The information shall be made available in an electronic form usable by consumers.

12 U.S.C. § 5533(a). As stated in the Senate's section-by-section analysis of the Dodd-Frank Act, "This section ensures that consumers are provided with access to their own financial information." S. Rep. No. 111-176, at 173 (2010).

51. From the outset of its Proposed Rule, the Bureau all but admitted it was seeking to achieve an objective far beyond the scope of Section 1033. "*In addition* to ensuring consumers can access covered data in an electronic form from data providers," the Bureau stated, it was also proposing to "address" what it perceived as "the challenges . . . with respect to the open banking system by delineating the scope of data that third parties can access on a consumer's behalf, the terms on which data are made available, and the mechanics of data access." Proposed Rule at 74,799 (emphasis added).

52. Below, Plaintiffs describe the Bureau's rulemaking in four parts. First, Plaintiffs summarize the components of the Bureau's proposed framework that are relevant to this challenge. Second, Plaintiffs summarize the relevant comments submitted to the Bureau regarding its proposal. Third, Plaintiffs describe the partial final rule the Bureau adopted regarding how it would recognize "standard setters" under its new regime. Finally, Plaintiffs explain how, despite the comments the Bureau received, it nonetheless adopted a Final Rule that retains the unlawful and harmful aspects of the Proposed Rule.

A. The Bureau's Proposed Rule

53. The Bureau issued its Proposed Rule on October 31, 2023. As the core mandate underlying its attempt to install a new regulatory regime governing open banking, the Proposed Rule required banks to "maintain a consumer interface" and "establish and maintain a developer interface" through which consumers' financial information could be shared with consumers and a broad range of third parties. Proposed Rule at 74,870 (proposed 12 C.F.R. 1033.301(a)).

1. Required Disclosure to "Authorized Third Parties"

54. As its core requirement, the Proposed Rule stated that a "data provider"—*i.e.*, a bank—"must 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, in an electronic form usable by consumers and authorized third parties." Proposed Rule at 74,870 (proposed 12 C.F.R. 1033.201(a)) (emphasis added). This requirement tracked the language of Section 1033 *except* for the significant addition of the term "authorized third parties," which does not appear in Section 1033. The Proposed Rule would require banks to provide consumer data to these third parties through the "developer interface" it required data providers to establish and maintain. *Id.*; *see generally*, Proposed Rule at 74,870-873 (Subpart C—Data Provider Interfaces; Responding to Requests) (proposed 12 C.F.R. 1033.301, 1033.321, 1033.331, 1033.341, 1033.351).

55. The Proposed Rule defined an "authorized third party" as any entity that complied with certain procedures for obtaining the consumer's informed consent—

procedures that *banks* would be tasked with ensuring the third party had followed. Proposed Rule at 74,869, 74,873 (proposed 12 C.F.R. 1033.131, 1033.401). These procedures included (i) providing the consumer with details about what information from the consumer's bank account the third party seeks to access and why; (ii) obtaining the consumer's express informed consent to such access; (iii) agreeing to abide by a series of obligations set forth in the Proposed Rule on how the third party would collect, use, and retain the consumer's data; and (iv) advising how the consumer could revoke the third party's access. *Id.* at 74,873 (proposed 12 C.F.R. 1033.401, 1033.411, 1033.421). The proposal expressly permitted the third party to use a data aggregator to perform these authorization procedures on its behalf, so long as the customer is advised of the data aggregator's involvement and the data aggregator agrees to the same obligations as the authorized third party. *Id.* at 74,874 (proposed 12 C.F.R. 1033.431). The consumer had no ability to select a different aggregator to facilitate the transfer of data.

56. After satisfying those authorization procedures, the authorized third party may collect, use, and retain the consumer's data to the extent "reasonably necessary to provide the consumer's requested product or service." *Id.* (proposed 12 C.F.R. 1033.421(a)(1)). The third party was then permitted to use and retain the consumer's data for the longer of (i) up to a year after the most recent authorization form was obtained, or (ii) as long as necessary to continue providing the consumer's requested product. *Id.* at 74,873-74 (proposed 12 C.F.R. 1033.421(b)(3), (b)(4)(ii)).

57. The Proposed Rule would then allow that authorized third party to share the consumer's data with *other* third parties, provided that the first third party "require[s] the

other third party by contract to comply with the" rules governing third-party data access and use. *Id.* at 74,874 (proposed 12 C.F.R. 1033.411(f)).

58. The Bureau did not explain why it was interpreting Section 1033 to allow such a broad swath of third parties to obtain customers' sensitive financial information. After citing the general statutory definition of "consumer" as including "an agent, trustee, or representative," 12 U.S.C. § 5481(4)), the Bureau simply asserted *ipse dixit* that the statute grants the Bureau "authority to establish a framework that readily makes available covered data in an electronic form usable by consumers *and third parties acting on behalf of consumers*, upon request." Proposed Rule at 74,802 (emphasis added). But it did not explain why it thought that any "third part[y] acting on behalf of consumers" would qualify as an "agent, trustee, or representative" of a consumer—terms that indicate a fiduciary-like relationship with an ongoing duty of loyalty to the consumer.

59. Notably, the Bureau had not always thought this interpretation was clear: in its advance notice of proposed rulemaking, the Bureau asked, "Who should be considered 'an agent, trustee, or representative' of an individual consumer for purposes of implementing section 1033 access rights?" Advance Notice of Proposed Rulemaking Regarding Consumer Access to Financial Records, 85 Fed. Reg. 71,003, 71,010 (Nov. 6, 2020). The Proposed Rule did not address comments the Bureau had received or explain its reasoning in answering this question so broadly.

2. The "Covered Data" Banks Must Share

60. The Proposed Rule required banks to make "covered data" available to any authorized third party. Proposed Rule at 74,870 (proposed 12 C.F.R. 1033.201). It defined

covered data to include certain information about the customer's account(s) with the bank, such as information pertaining to transaction history and pending transactions, account balances, upcoming bill information, and account verification information. *Id.* (proposed 12 C.F.R. 1033.211). Covered data also included "terms and conditions" associated with the account, which generally mean the contract terms between the data provider and the consumer, such as "the applicable fee schedule," interest rates, "rewards program terms," and whether the consumer "opted into overdraft coverage" or "entered into an arbitration agreement." *Id.* (proposed 12 C.F.R. 1033.211(d)).

61. The Proposed Rule also required banks to share an additional category of "covered data" defined in terms of its functionality, rather than information about the customer's product. Specifically, the Proposed Rule would require banks to share "[i]nformation to initiate payment" from an account, which "includes" a consumer's account and routing number in either tokenized or non-tokenized form. *Id.* (proposed 12 C.F.R. 1033.211(c)). The Bureau did not address the unique risks posed by the sharing of payment-initiation information, particularly when shared on the scale of potentially tens of millions of consumers with thousands of third parties. Nor did the Proposed Rule draw any distinction in treatment for this information, instead requiring that it be shared on the same terms as any other information about a consumer's account.

62. The Bureau did not acknowledge (much less distinguish) its prior guidance recognizing an important difference between "[a]uthorized data access" and "payment authorization." *See* CFPB, *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation*, 4 (Oct. 18, 2017),

https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf ("Authorized data access, in and of itself, is not payment authorization. Product or service providers that access information and initiate payments obtain separate and distinct consumer authorizations for these separate activities.").

3. Ensuring Third-Party Security

63. Although the Bureau proposed to require banks to share customers' most sensitive financial information with countless third parties, the Proposed Rule did not expressly provide *any* role for the Bureau to play in ensuring that those third parties' security practices are sufficiently robust or even that they comply with the same requirements imposed on banks by the Proposed Rule. Instead, the Bureau generally tasked *banks* with that role—while at the same time limiting banks' tools for fulfilling it.

64. *First*, the Proposed Rule provided that the mandate that banks "*must* make available covered data" is triggered whenever the bank receives information from a third party that "[c]onfirm[s] the third party has followed the authorization procedures" prescribed by the Proposed Rule." Proposed Rule at 74,871 (proposed 12 C.F.R. 1033.331(b)(1)(i)-(iii) (emphasis added)).

65. *Second*, the Proposed Rule sought to circumscribe in numerous ways banks' ability to deny third parties' access to the developer interface based on risk-management concerns.

66. For starters, the Proposed Rule deemed a denial of access to be "not unreasonable" if the denial was "necessary to comply with" the bank's obligations under relevant provisions of the Federal Deposit Insurance Act or the Gramm-Leach-Bliley Act.

Proposed Rule at 74,871 (proposed 12 C.F.R. 1033.321(a)). Troublingly, the Bureau did not specify who would determine what is "necessary," nor did it address the untenable choice banks with risk-management concerns would be put to: deny access on safety-and-soundness grounds and risk enforcement by the CFPB for *overly restrictive* access policies, or allow access based on the Proposed Rule and risk enforcement by prudential regulators for *overly lax* policies. *Id.*

67. The Proposed Rule recognized that a bank may also "*reasonably* deny[]" access on risk-management grounds, *id.* (proposed 12 C.F.R. 1033.321(a) (emphasis added)), but provided that a denial would be considered reasonable only if, "at a minimum," the denial is "directly related to a specific risk of which the data provider [was] aware." *Id.* (proposed 12 C.F.R. 1033.321(b)). The Proposed Rule did not specify or give any illustrative examples of what constitutes a "specific" risk or how serious such a risk must be. Nor did the CFPB explain how this standard interacted with its additional caveat that access could be denied if "the third party does not present evidence that its data security practices are adequate to safeguard the [consumer's] data." *Id.* (proposed 12 C.F.R. 1033.321(d)(1)).

68. The Proposed Rule vaguely warned that such risk-based denials must be carried out "in a consistent and non-discriminatory matter," a hazy and subjective standard that leaves banks with no assurance that a denial based on legitimate risk-management concerns—even those deemed necessary to meet expectations of its primary financial regulator—would not expose it to an enforcement action by the Bureau. *Id.* (proposed 12 C.F.R. 1033.321(b)). Instead, banks making risk-management decisions must wonder whether a legitimate denial of access will ultimately leave them exposed if the CFPB

concludes that a bank previously granted what the Bureau perceives as a materially similar request.

69. *Third*, puzzlingly, the Bureau did not require that all authorized third parties use the new developer interface that banks would be required to establish and maintain. Nor did it ban the riskiest method of accessing customer financial data: screen scraping. The Bureau repeatedly acknowledged "screen scraping's inherent overcollection, accuracy, and consumer privacy risks," Proposed Rule at 74,813; that "screen scraping creates data security, fraud, and liability risks for data providers," *id.* at 74,854; and that there is "nearly universal consensus that developer interfaces should supplant screen scraping," *id.* at 74,798. Yet the Proposed Rule did not actually ban screen scraping despite its acknowledged risks; it assumed that "the market [will] move away from screen scraping" based on the onerous obligations put on data providers regarding developer interfaces. *Id.* Banks, by contrast, are required to walk a very fine line: the Proposed Rule further warned that the Bureau would "evaluate whether data providers are blocking screen scraping without a bona fide and particularized risk management concern" during the implementation period; if so, the Bureau would "consider using the tools at its disposal to address this topic ahead of the proposed compliance dates." *Id.* at 74,800.

70. *Finally*, having compelled broad sharing of consumers' most sensitive information, required banks to assume primary responsibility for managing the risks of that sharing, and at the same time limited banks' authority to mitigate those risks, the Proposed Rule declined to articulate any limitations on banks' liability if customer data is breached. The Bureau rejected proposals to ensure that liability for data misuse or

compromise when data is in the hands of a third party should rest with that third party. Instead, the Proposed Rule left banks exposed to unspecified and unpredictable potential liability for data breaches that could have been avoided only by denying third parties access to their API in the first place, not to mention complaints by fintech companies and potential Bureau enforcement actions. *See, e.g.*, U.S. Bank, Comment Letter on Rule, Docket No. CFPB-2023-0052, at 3 (Dec. 27, 2023), https://www.regulations.gov/comment/CFPB-2023-0052-0795.

4. Standard Setters

71. Having already proposed to task data providers with overseeing the security and compliance of purportedly authorized third parties, the Bureau also proposed to delegate to private organizations much of its claimed authority to set substantive standards for compliance with the Rule.

72. In addition to employing standard-setting organizations to provide technical requirements, such as the appropriate format in which to present data, the Bureau also proposed to give private standard setters a significant role to play in measuring banks' compliance with substantive and policy-oriented requirements. For example, the Bureau proposed to look to private organizations to set "qualified industry standard[s]" for:

- how much "scheduled downtime [of the API] may be reasonable," Proposed Rule at 74,871 (proposed 12 C.F.R. 1033.311(c)(1)(i)(C));
- whether "any frequency restrictions" on the number of requests a bank will process through its developer interface "are reasonable," *id.* (proposed 12 C.F.R. 1033.311(c)(2));

- whether a bank's "method to revoke any third party's authorization" is "reasonable," *id.* at 74,872 (proposed 12 C.F.R. 1033.331(e));
- whether "a data provider's policies and procedures regarding accuracy [of information it provides] are reasonable," *id.* at 74,873 (proposed 12 C.F.R. 1033.351(c)(3)); and
- whether a bank's risk-management-related denial of access to the developer interface was "reasonable," *id.* at 74,871 (proposed 12 C.F.R. 1033.321(c)).

73. For these substantive requirements, the Bureau generally proposed that a regulated party's "adherence to a qualified industry standard" would constitute "[i]ndicia" that the data provider had complied with its obligations under the Proposed Rule. *See, e.g.*, *id.*

74. The Proposed Rule did not identify anything in the statute that permitted the Bureau to delegate the formulation of substantive policy "standards" to private organizations. To explain its decision, the Bureau pointed to the "granular coding and data requirements" involved in developing the interfaces that "risk[] becoming obsolete almost immediately," which led the Bureau to prefer the "efficient evolution of technical standards" that external standard-setting organizations facilitate better than government agencies. Proposed Rule at 74,801. But that plainly does not explain why private organizations should have a role in setting compliance standards for substantive regulatory requirements that go far beyond coding data, such as whether a bank's risk-management determinations are "reasonable" or its policies and procedures were appropriate. *Id.*

5. Compliance Deadlines

75. Despite the substantial new obligations the Proposed Rule would impose, the Bureau proposed to give the largest banks—depository institutions with at least $500 billion in total assets and nondepository institutions that generated $10 billion in revenue in 2023 or expect to in 2024—a mere six months after publication of the final rule in the Federal Register to come into compliance. Proposed Rule at 74,869 (proposed 12 C.F.R. 1033.121(a)).

76. In addition to the unreasonably short deadline, the Proposed Rule did not explain why the Bureau did not propose to key the compliance deadlines off of the promulgation of standards by the standard-setting organizations it proposed to recognize. As commenters pointed out, that failure would pose challenges because "some of the industry standards mentioned by the CFPB do not yet exist, and they will not exist until qualified industry body(s) are recognized and publish such standards." JPMC Cmt. Ltr., *supra* ¶ 11, at 31.

6. Access-Fee Prohibition

77. Finally, the Bureau proposed to forbid data providers from "impos[ing] any fees or charges on a consumer or an authorized third party" to compensate for establishing or maintaining its interfaces or processing requests for consumers' data. Proposed Rule at 74,870 (proposed 12 C.F.R. 1033.301(c)). In other words, banks would be required to provide the extensive services mandated by the Proposed Rule—including the significant oversight, compliance, and liability costs—for free. According to the Bureau, the fee prohibition is "necessary . . . to effectuate consumers' rights" under Section 1033 to receive

their data "upon request." *Id.* at 74,814. But the Bureau did not square that explanation with its later acknowledgement that banks may still indirectly lawfully "pass[] on to consumers" some of the costs of their APIs in the form of, for instance, "higher account fees." *Id.* at 74,853. Nor did the Bureau explain why consumers should bear the costs of significantly expanded third-party access to their data, rather than the third parties that directly benefit from that access.

78. The Bureau proposed this prohibition on banks even recouping their costs from third parties despite recognizing the immense costs of compliance. The Bureau itself cited a median annual cost of maintaining a developer interface of $21 million (or $210 million over a decade), which ranged as high as $47 million annually for certain banks. *Id.* at 74,847-48. As commenters explained, even these estimates "vastly underestimate[d] the amount of work that even the largest and most technologically advanced" banks would "have to undertake to achieve compliance." BPI & TCH Cmt. Ltr., *supra* ¶ 8, at 14, 67-68. And the CFPB proposed no corresponding prohibition on third parties' charging fees related to their data access and transmission, or the products or services they provide using that data.

B. The Comment Period

79. The Bureau received more than 11,000 comments on its Proposed Rule. The comments were submitted by a range of financial-services institutions, consumer organizations, and public-interest groups. A number of commenters raised serious concerns about the Proposed Rule, such as (among many others):

- **Teller, Inc.:** The Proposed Rule exceeds the CFPB's authority by attempting to turn a "modest provision intended to provide 'consumer rights to access information'" and turning into a license to "reinvent consumer banking" by "inaugurat[ing] 'open banking' in the United States." Teller, Inc., Comment Letter on Rule, Docket No. CFPB-2023-0052, at 1-2 (Dec. 30, 2023), https://www.regulations.gov/comment/CFPB-2023-0052-0903 (Teller Cmt. Ltr.). In particular, third parties are not "consumer[s]" within the meaning of the statute, and the Bureau thus cannot compel dissemination of consumers' financial information to them. *See id.* at 8-12.
- **Credit One:** The Proposed Rule "creates significant risk for consumers' sensitive financial data to be exposed to bad actors" and "appears to place unfair burdens on financial institutions," including "to ensure third parties have followed [appropriate] authorization procedures." Credit One, Comment Letter on Rule, Docket No. CFPB-2023-0052, at 1 (Jan. 2, 2024), https://www.regulations.gov/comment/CFPB-2023-0052-0953. The Bureau should also ensure third parties are "held to the same exacting standards that regulated financial institutions are held to" with respect to data protection. *Id.* at 2. The Proposed Rule is also deficient because it fails to "expressly prohibit . . . screen scraping." *Id.*
- **JPMorgan Chase & Co.:** The Proposed Rule inappropriately relies on standard setters for many choices that "tend to be in the spirit of regulatory enforcement," such as caps on frequency with which data may be accessed,

the level of accuracy in responses that data providers must maintain, and permissible amount of platform downtime. JPMC Cmt. Ltr., *supra* ¶ 11, at 16-17. The Proposed Rule also exceeds the CFPB's authority insofar as it would require banks to share information to initiate payment from a Regulation E account. *Id.* at 8-11.

- **BPI & TCH:** The Proposed Rule's use of standard setters could result in privately promulgated qualified industry standards receiving "extraordinary weight by market participants." BPI & TCH Cmt. Ltr., *supra* ¶ 8, at 13. Reliance on standard-setters should be abolished with respect to certain provisions such as the permissible total amount of API downtime and access restrictions. *Id.* at 37. Moreover, "the fee prohibition . . . is not grounded in the statutory text." *Id.* at 42.
- **Consumer Bankers Association:** The CFPB lacks legal authority for the Proposed Rule because Section 1033's "plain statutory language is fundamentally centered on a consumer's right to access their own information." Consumer Bankers Ass'n, Comment Letter on Rule, Docket No. CFPB-2023-0052, at 9 (Dec. 29, 2023), https://www.regulations.gov/comment/CFPB-2023-0052-0951. To the extent the Bureau can prescribe rules, rather than rely on standard setters, the Bureau itself should clarify the content of certain requirements the Proposed Rule would impose, such as what would constitute an "unreasonable" restriction on the frequency of data

requests. *Id.* at 18. And the Bureau should allow reasonable fees to be charged to authorized third parties. *Id.* at 15-17.

- **American Bankers Association:** The proposed rule's "prohibition on fees" is "unsupported by law" and "represents nothing less than a forced transfer of value" from data providers to "data aggregators and third parties seeking to monetize the information." Am. Bankers Ass'n, Comment Letter on Rule, Docket No. CFPB-2023-0052, at 4, 11 (Jan. 2, 2024), https://www.regulations.gov/comment/CFPB-2023-0052-0962. The proposed rule also presents grave security risks because, instead of CFPB oversight of risk management, "far too many portions of the [proposed rule] are reliant on data providers or standard-setting bodies." *Id.* at 5.

80. Based on these concerns, commenters called for rescission of the Rule or at least substantial changes to numerous key elements of the Proposed Rule. *See, e.g.*, Teller Cmt. Ltr., *supra* ¶ 79.

C. The Final Rule Regarding Standard Setters

81. On June 11, 2024, the CFPB finalized a portion of its Proposed Rule concerning standard setters. In particular, the CFPB published the procedures by which it would recognize external standard-setting bodies, whose "consensus standards" the Bureau proposed to rely on in interpreting various provisions of the Rule. *See* Industry Standard Setting, 89 Fed. Reg. 49,084 (June 11, 2024) (to be codified at 12 C.F.R. 1033.101, 1033.131, 1033,141), https://www.govinfo.gov/content/pkg/FR-2024-06-11/pdf/2024-12658.pdf (Standard-Setter Rule).

82. In the Standard-Setter Rule, the Bureau explained that it would select standard-setting organizations via application based on a number of characteristics, such as the organization's openness to all interested parties, balancing decision-making power among all interested parties, transparency with respect to procedures, operation by consensus, and a system of entertaining objections and appeals that comports with due process. *See* Standard-Setter Rule at 49,091.

83. In response to comments questioning the Bureau's authority to recognize standard setters at all, it cited a series of statutory provisions that delegate certain rulemaking authority *to the Bureau*. *See id.* at 49,086 (citing 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. § 5533(d) (similar); 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). The Bureau did not identify any statutory provision giving the Bureau authority to delegate its rulemaking authority to private organizations.

84. The Standard-Setter Rule also repeated the Bureau's rationale for delegating policy standards to standard-setting bodies—that "very granular technical requirements could rapidly become obsolete" if prescribed by regulators, "while industry-led standard-setting would be better able to keep pace with changes in the market and technology" if the standard setters had been recognized pursuant to fair and appropriate procedures. *Id.* at 49,084.

D. The Final Rule Challenged In This Case

85. The Bureau issued the Final Rule on October 22, 2024.

86. Despite the numerous objections raised during the comment period, the Bureau persisted in finalizing a rule that not only retains largely all the fundamentally problematic aspects of the proposed rule, but even exacerbates some commenters' concerns.

87. First, the Rule still compels disclosure of customers' information to any "authorized third parties," which is defined broadly to include any third-party company that purportedly completes authorization procedures prescribed in the Rule.

88. Second, the Rule persists in implementing an unsafe and irrational regulatory framework. The Bureau continued to:

- require the sharing not only of data about the customer's account, but of "information to initiate payment" in or out of the customer's account, Final Rule at 567 (to be codified at 12 C.F.R. 1033.211(c));
- decline to assert a clear role for itself in ensuring third parties' compliance with authorization procedures, instead vaguely relying on banks to "document" such compliance, *id.* at 576 (to be codified at 12 C.F.R. 1033.331(b));
- impose significant limits on banks' ability to engage in risk-management-based denials of access to third parties, even in the event that banks deny such access because of the "safety and soundness standards of a prudential

regulator," which is not a sufficient basis to deny access, *id.* at 574-75 (to be codified at 12 C.F.R. 1033.321(a), (b));

- refuse to require third parties to use the new developer interfaces or ban screen scraping, *see id.* at 318-19; and
- refuse to set forth any rules for fairly apportioning liability among data providers, authorized third parties, and data aggregators in the event a customer's data is breached or misused, in light of the unsafe framework the CFPB had created.

89. Third, the Rule continues to outsource substantial policymaking authority to private standard-setting organizations. Far from looking to private standard-setters for only "granular technical requirements," Standard-Setter Rule at 49,084, the Rule delegates broad authority to define such substantive compliance issues as what constitutes "reasonable" denial of interface access on risk-management grounds or "reasonable" amounts of downtime, access limits, and other similar substantive issues, including those over which prudential bank regulators exercise substantial control and oversight authority. Final Rule at 571-74 (to be codified at 12 C.F.R. 1033.311(c), 1033.311(d), 1033.321(c)).

90. Fourth, the Bureau persisted in setting an arbitrary and irrational compliance schedule based on dates certain, rather than the issuance of "consensus standards" by standard-setting organizations. On the date the Bureau unveiled the Final Rule, it had not yet recognized a single qualified standard-setting organization. It did not state when any such recognition would occur, let alone when any such organization would actually issue *any* of the numerous consensus standards that the Bureau made critical to

compliance with the Rule. As a result, the compliance clock is ticking now, despite data providers having no knowledge of what "consensus standards" they might need to build to compliance with.

91. Finally, notwithstanding the enormous burdens and costs described above, the Rule continues to prohibit banks from charging *any* fees to authorized third parties and data aggregators to compensate for the costs of establishing and providing access through banks' APIs mandated by the Rule. Final Rule at 570 (to be codified at 12 C.F.R. 1033.301(c)).

CLAIMS FOR RELIEF

COUNT I
Administrative Procedure Act
(In Excess of Statutory Authority – Unlawful Interpretation of "Consumer")
5 U.S.C. § 706

92. Plaintiffs repeat and incorporate by reference all the allegations set forth above.

93. Under the APA, the Court "shall . . . hold unlawful and set aside" final agency action found to be "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right." 5 U.S.C. § 706(2)(C).

94. The Rule is final agency action "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right" because the Bureau does not have authority to compel provision of covered data to "authorized third parties" who are not the consumer, or at least in an agency or fiduciary-type relationship with the consumer. *Id.*

95. Section 1033 requires a bank to provide the *consumer*, "upon request," with information about financial products or services the *consumer* is obtaining from the bank. *See* 12 U.S.C. § 5533(a). The purpose of this provision is to keep consumers informed about their own financial products and services. That is confirmed by the structure of the Dodd-Frank Act, as Section 1033 is sandwiched between a provision requiring periodic affirmative disclosures "*to consumers*" about the risks and benefits of their financial products, 12 U.S.C. § 5532(a) (emphasis added), and a provision concerning banks' "response *to consumers*" regarding "complaints" or "inquiries," 12 U.S.C. § 5534(a) (emphasis added), neither of which plausibly contemplates obligations to potentially thousands of third-party fintech companies or data aggregators. And it is also confirmed by the legislative history of Section 1033 itself, which unambiguously states that the provision "ensures that consumers are provided with access to their own financial information." S. Rep. No. 111-176, at 173 (2010).

96. The general definitional provision cited by the Bureau does not alter this plain textual meaning. At the beginning of the Consumer Financial Protection Act of 2010 (Title X of Dodd-Frank), the Act defines "consumer" as "an individual or an agent, trustee, or representative acting on behalf of an individual." 12 U.S.C. § 5481(4). But that definition does not authorize the Bureau to mandate that banks share consumer data with any "authorized third party." Companies that establish arm's-length commercial relationships with consumers are neither agents, nor trustees, nor representatives of those consumers within the meaning of this definition. Those words, which are themselves undefined, are

legal terms of art that are presumed to take their established, common-law meaning. *Evans* v. *United States*, 504 U.S. 255, 259 (1992).

97. 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 (Am. Law Inst. 2006); Restatement (Third) of Trusts § 2 (Am. Law Inst. 2003). Fintech companies and data aggregators do not quality as agents or trustees. That leaves only the term "representative," which must be understood "by the company it keeps." *See McDonnell* v. *United States*, 579 U.S. 550, 569 (2016) (internal quotation omitted).

98. Although the term "representative" may have a broader meaning in some contexts, here that term must be interpreted as similar in nature to an "agent" or "trustee"—*i.e.*, to mean a third party that has a special, fiduciary-like relationship with or duty of loyalty to the consumer. *See, e.g.*, *Dubin* v. *United States*, 599 U.S. 110, 124-127 (2023). Accordingly, in this statute, a "representative" means "someone who represents another as agent, deputy, substitute, or delegate" and is typically "invested with the authority of the principal." *Representative*, Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/representative (accessed Oct. 21, 2024). Fintech companies and data aggregators seeking to profit off of consumers' financial data in exchange for providing a discrete product or service do not have any of those characteristics, and cannot be considered a customer's financial "representative" simply because the customer authorized limited access in order to obtain the product or service.

99. For these reasons, the Bureau's promulgation of the Rule was in excess of statutory jurisdiction, authority, or limitations. Plaintiffs are therefore entitled to relief pursuant to 5 U.S.C. §§ 702, 706, and the Rule should be held unlawful and set aside.

COUNT II
Administrative Procedure Act
(Arbitrary and Capricious – Failure to Engage in Reasoned Decisionmaking by Placing Consumer Data At Risk)
5 U.S.C. § 706

100. Plaintiffs repeat and incorporate by reference all the allegations set forth above.

101. Under the APA, the Court "shall . . . hold unlawful and set aside" final agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A).

102. The Rule is final agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law" because the Bureau adopted a fundamentally irrational regulatory framework that increases the risk of misuse or compromise of consumer data while reducing protections that banks could afford to that data.

103. Requiring banks to share their customers' financial data with third-party commercial actors, with limited and ill-defined ability to deny access, necessarily increases the risk of compromise of that data. That is particularly true given that these third parties have no fiduciary relationship or duty of loyalty to consumers, nor are they comprehensively regulated for security as banks are. Yet the Bureau's framework is set up to maximize that risk while reducing protections against it. Viewed as a whole, that

framework amounts to arbitrary and capricious rulemaking. *See 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).

104. First, the Bureau unjustifiably required banks not only to share information about the customer's account, but information sufficient to initiate a payment from a consumer's account.

105. Second, despite commenters' pleas, the Bureau chose not to mandate that third parties use the developer interfaces when available rather than use screen-scraping, notwithstanding its acknowledgement (and the near-universal agreement) that the latter practice poses unacceptable risks to consumers.

106. Third, the Bureau declined to assume responsibility for assessing and verifying these third-party actors' security practices and compliance before they are permitted to access consumers' data. Instead, the Bureau deputized banks to fulfill those functions. The Rule vaguely requires banks to "document" that the third parties have complied with the Rule. And while it purports to expressly authorize banks to determine that third-party security practices are inadequate, that authority is sufficient to justify a denial of access only if the third party "does not present *any* evidence that its information security practices are adequate to safeguard the covered data." Final Rule at 575 (to be codified at 12 C.F.R. 1033.321(d)).

107. Fourth, inserting itself into an essential banking function, the Bureau placed limits on banks' ability to manage the risks of their business by denying any particular third party's access to its developer interface. In particular, the Bureau prescribes an overly

demanding standard for when a risk-management-based denial is permissible, relies on standard setters to give content to this paradigmatically regulatory issue related to safety and soundness, and imposes an ill-explained "consisten[cy]" requirement for access denials that will hamstring banks that may have to make thousands of risk-management decisions daily in connection with these APIs. Notably, all of these limitations apply *even if* the bank denies access pursuant to policies and procedures that further the safety and soundness standards of its prudential regulators.

108. These features create a framework that unacceptably puts consumers' sensitive financial data at risk and hobbles banks in their ability to protect that data. Yet the Bureau nonetheless declined to address the serious liability concerns that its regime creates. Specifically, the Bureau failed to set rules for which parties will bear liability (and under what circumstances) when a consumer's financial data is compromised under the broad sharing regime it mandated.

109. The Bureau's approach of forcing banks to share their customers' most sensitive data and then potentially leaving banks holding the bag when that data is misused or compromised is arbitrary and capricious and fundamentally unfair.

110. For these reasons, the Bureau's promulgation of the Rule was arbitrary and capricious. Plaintiffs are therefore entitled to relief pursuant to 5 U.S.C. §§ 702, 706, and the Rule should be held unlawful and set aside.

COUNT III
Administrative Procedure Act
(In Excess of Statutory Authority – Compulsory Provision of Payment-Initiation Information)
5 U.S.C. § 706

111. Plaintiffs repeat and incorporate by reference all the allegations set forth above.

112. Under the APA, the Court "shall . . . hold unlawful and set aside" final agency action found to be "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right." 5 U.S.C. § 706(2)(C).

113. The Rule is final agency action "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right," *id.*, because the Bureau does not have authority to compel banks to provide to third parties "[i]nformation to initiate payment to or from a Regulation E account," Final Rule at 567 (to be codified at 12 C.F.R. 1033.211(c)).

114. Section 1033 requires banks to provide information about a customer's account: "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). Consistent with Section 1033's focus on providing "information" to customers, each of the specific listed terms—transactions, costs, charges, and usage data—constitutes a piece of descriptive data about an account's activity, features, or characteristics.

115. But the Rule goes beyond the statute by requiring disclosure of a fundamentally different piece of information: information "to initiate payment." Final Rule at 567 (to be codified at 12 C.F.R. 1033.211(c)). That goes beyond the scope of Section 1033. Section 1033 authorizes the sharing of information *about* a financial product or service. Yet

the Bureau has impermissibly crafted this category of covered data to enable a specific *functionality*: payment initiation by third parties. Those are two different things. As even the Bureau itself has previously recognized, "[a]uthorized data access . . . is not payment authorization." *See* CFPB, *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation*, 4 (Oct. 18, 2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

116. Section 1033 does not authorize the Bureau to require banks to facilitate any particular functionality for third parties, let alone functionality that would allow third parties to directly move customers' money out of their accounts.

117. For these reasons, the Bureau's promulgation of the Rule was in excess of statutory jurisdiction, authority, or limitations. Plaintiffs are therefore entitled to relief pursuant to 5 U.S.C. §§ 702, 706, and the Rule should be held unlawful and set aside.

COUNT IV
Administrative Procedure Act
(In Excess of Statutory Authority – Unlawful Delegation of Regulatory Authority to Private Standard Setters)
5 U.S.C. § 706

118. Plaintiffs repeat and incorporate by reference all the allegations set forth above.

119. Under the APA, the Court "shall . . . hold unlawful and set aside" final agency action found to be "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right." 5 U.S.C. § 706(2)(C).

120. The Rule is final agency action "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right" because nothing in the statute purports to authorize delegation of the Bureau's regulatory authority to a private actor. *Id.*

121. The Bureau has relied on a number of statutory provisions that empower *the Bureau* to prescribe rules. Standard Setter Rule at 49,086 (citing 12 U.S.C. § 5533(a) (information shall be made available to consumers "[s]ubject to rules *prescribed by the Bureau*") (emphasis added); § 5533(d) (similar); § 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)). But none of those provisions even hints at the possibility of the Bureau outsourcing those rulemaking directives to private organizations. The Bureau explained that it believed private standard setters could better modify granular technical requirements for standardized data formats as technology evolves, *see id.* at 49,084, but that is no justification for delegating responsibility for establishing standards of substantive compliance—such as what kinds of risk-management denials are "reasonable"—to private organizations.

122. Nor does the statute authorize such delegation to standards-setting organizations. Reliance on private parties to prescribe standards of substantive law raises serious constitutional concerns regarding the impermissible congressional delegation of legislative power, and therefore is permissible only with "express congressional authorization." *Consumers' Research* v. *FCC*, 109 F.4th 743, 777 (5th Cir. 2024) (en banc). As noted above, there is no such authorization in Section 1033.

123. For these reasons, the Bureau's promulgation of the Rule was in excess of statutory jurisdiction, authority, or limitations. Plaintiffs are therefore entitled to relief pursuant to 5 U.S.C. §§ 702, 706, and the Rule should be held unlawful and set aside.

COUNT V
Administrative Procedure Act
COUNT VI(Arbitrary and Capricious – Failure to Engage in Reasoned Decisionmaking with Respect to Compliance Deadlines)
5 U.S.C. § 706

124. Plaintiffs repeat and incorporate by reference all the allegations set forth above.

125. The APA requires a reviewing court to hold unlawful and set aside any agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A).

126. The Rule is final agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law" with respect to its compliance timelines because under the APA, an agency must explain deadlines it selects, including for compliance. *See Wynnewood Refin. Co.* v. *EPA*, 77 F.4th 767, 782-783 (D.C. Cir. 2023); *Piedra-Alvarez* v. *Barr*, 829 Fed. App'x 833, 834 (9th Cir. 2020).

127. Here, the Bureau set a compliance timeline that is fundamentally irrational because it is not tied to the promulgation of the consensus standards that the Bureau has made fundamental to compliance with the Rule. Those standards, once promulgated, will naturally (and by the Bureau's apparent design) become the industry's default standard for compliance with the relevant obligations under the Rule. But banks cannot build toward compliance with standards that do not exist. And until such standards are promulgated,

any steps data providers take toward compliance come with the substantial risk that of being wasted in the event that they must unwind and redo that work to adapt to standards. Left to wait some indeterminate amount of time before they can take meaningful steps toward compliance, data providers are nonetheless staring down the certain deadlines the CFPB has prescribed.

128. For these reasons, the Bureau's promulgation of the Rule was arbitrary and capricious with respect to the prescribed compliance periods. Plaintiffs are therefore entitled to relief pursuant to 5 U.S.C. §§ 702, 706, and the compliance deadlines should be held unlawful and set aside.

COUNT VII
Administrative Procedure Act
(In Excess of Statutory Authority – Access-Fee Ban)
5 U.S.C. § 706

129. Plaintiffs repeat and incorporate by reference all the allegations set forth above.

130. Under the APA, the Court "shall . . . hold unlawful and set aside" final agency action that is "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right." 5 U.S.C. § 706(2)(C).

131. The Rule is final agency action "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right" because the Bureau does not have authority to prohibit banks from charging reasonable fees to third parties or data aggregators to access banks' APIs. *Id.* Nothing in the text or structure of Section 1033 prohibits banks from charging reasonable access fees, even to cover their costs. When Congress intends to

mandate provision of a product or service at no cost, it knows how to achieve that result. *See, e.g.*, 15 U.S.C. § 1681c-1(a)(2)(B) (Fair Credit Reporting Act requirement that consumer reporting agencies must provide to consumers all required disclosures "without charge to the consumer"). Notably, it even did so elsewhere in Dodd-Frank. *See* 15 U.S.C. § 1691(e)(4) (Creditors shall provide copies of written appraisals or valuations "at no additional cost to the applicant."); 15 U.S.C. § 1639h(c) (requiring creditors to provide a copy of certain appraisals "without charge").

132. Nor does Section 1033 implicitly delegate to the Bureau the authority to ban banks from charging reasonable access fees, thus providing a windfall to fintechs and data aggregators. Although Section 1033 broadly contemplates "rules prescribed by the Bureau," 12 U.S.C. § 5533(a), interpreting such vague language to authorize federal agencies to determine when businesses are allowed to charge for providing services in a competitive area would raise serious concerns under the U.S. Constitution about the impermissible delegation of legislative power.

133. For these reasons, the Bureau's promulgation of the Rule was in excess of statutory jurisdiction, authority, or limitations. Plaintiffs are therefore entitled to relief pursuant to 5 U.S.C. §§ 702, 706, and the Rule should be held unlawful and set aside.

PRAYER FOR RELIEF

Wherefore, Plaintiffs respectfully request that this Court enter judgment in their favor and against Defendants as follows:

(i) A declaratory judgment that the Rule is in excess of the Bureau's statutory authority within the meaning of the Administrative Procedure Act, *see* 5 U.S.C. § 706(2)(C);

(ii) A declaratory judgment that the Rule is arbitrary, capricious, or otherwise contrary to law within the meaning of the Administrative Procedure Act, *see* 5 U.S.C. § 706(2)(A);

(iii) An order setting aside the Rule in its entirety pursuant to the Administrative Procedure Act, *see* 5 U.S.C. § 706(2);

(iv) An order permanently enjoining Defendants from enforcing the Rule against Plaintiffs and their members;

(v) A declaratory judgment that the Rule's compliance deadlines are arbitrary, capricious, or otherwise contrary to law within the meaning of the Administrative Procedure Act, *see* 5 U.S.C. § 706(2)(A), (C), and an order vacating and setting aside the compliance deadlines, *see* 5 U.S.C. § 706(2);

(vi) A declaratory judgment that the Rule's prohibition on access fees is in excess of the Bureau's statutory authority, *see* 5 U.S.C. § 706(2)(C), arbitrary, capricious, or otherwise contrary to law within the meaning of the Administrative Procedure Act, *see* 5 U.S.C. § 706(2)(A), (C), and an order vacating and setting aside the prohibition on access fees pursuant to the Administrative Procedure Act, *see* 5 U.S.C. § 706(2);

(vii) An order issuing all process necessary and appropriate to delay the effective date and implementation of the Rule and the Standard-Setter Rule pending the conclusion of this case;

(viii) An order awarding Plaintiffs their reasonable costs, including attorneys' fees, incurred in bringing this action; and

(ix) Any other relief as the Court deems just and equitable.

Dated: October 22, 2024

/s/ John T. McGarvey /s/ M. Thurman Senn

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

John Court**
Paige Pidano Paridon**
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

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

* *Pro hac vice* pending
** *Pro hac vice* forthcoming

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