Platform Money

Raúl Carrillo†

The public rightly considers the traditional banking system expensive, slow, and unfair. In response, technology companies have developed an 'open banking' sector. They combine transaction data from financial institutions with other datasets to develop applications for additional financial services, including personalized financial management and credit underwritten by data that credit bureaus have not historically collected, such as cash flow data.

The open banking sector also includes companies like PayPal, Venmo, and Cash App, which offer "digital wallets" (smartphone applications) that store customer balances outside banks. These companies claim to enable free, faster, fairer balance transfers and payments. Roughly one in three Gen Xers, Millennials, and Gen Zers consider a wallet their primary checking account. However, the Federal Deposit Insurance Corporation does not insure the balances, and many scholars have argued that these business models undermine broader goals of banking regulation.

In this Article, I synthesize concerns based on banking law with concerns about data governance to promote a regulatory proposal for the Consumer Financial Protection Bureau (CFPB) to govern this digital wallet ecosystem and advance a new conceptual approach toward open banking.

I refer to stored digital wallet balances as "platform money" to highlight how technology companies are stacking data-intensive consumer applications on top of the U.S. banking system, profiting from its deficiencies, including deposit volatility and unenforceable entry restrictions.

I analyze the practices of "data brokers," which supply the infrastructure for transferring funds and data in the platform money ecosystem.

---

† Academic Fellow and Lecturer in Law, Columbia Law School. The Author thanks Nikita Aggarwal, Jeff Sovern, Rory Van Loo, and other participants in the March 2023 Consumer Law Conference at Berkeley Law School. The Author thanks Peter Conti-Brown, Howell Jackson, David Zaring, and other participants in the Fall 2022 Wharton School financial regulation workshop series. The Author thanks Talia Gillis, Will Thomas, and other participants in a virtual Summer 2022 Junior Scholars Research Workshop session. For helpful feedback in drafting the Article, the Author thanks Dan Awrey, Luke Herrine, Lenore Palladino, Nathan Tankus, Sandeep Vaheesan, and Arthur Wilmarth, Jr. For generative discussion in the initial formation of the Article, the Author thanks Yochai Benkler, Rohan Grey, Amy Kapczynski, Salomé Viljoen, and other members of a 2022 law and technology workshop held at Yale Law School.

Brokers use this data to profit in other markets, including credit reporting, identity management, and targeted advertising. They exercise platform power in ways that unnecessarily threaten the integrity of the traditional banking system and risk harm to consumers in the open banking system, including loss of funds, theft, identity fraud, and operational failure beyond the danger posed by previous practices in financial data usage, such as credit reporting. Unfortunately, background laws encase brokers from private challenges, while existing statutes and regulations do not sufficiently govern their business model or practices.

I argue the CFPB should prevent data brokers transferring funds between bank accounts and platform money apps from collecting, using, or retaining more data than is strictly necessary to transfer those funds in compliance with existing laws (such as laws against money laundering). I argue the risk platform money poses to consumers underscores the need for a revitalized 'regulated industries' approach promoting a continuum of public governance over critical networks, platforms, and utilities in new forms of consumer banking. This approach is crucial for ensuring cheaper, faster, fairer banking while avoiding emergent risks for the public.

Introduction

Consumers don't like their banks. The public rightly considers the traditional banking system slow, expensive, and unfair. Taking advantage of this dissatisfaction, major technology companies have developed an "open banking" sector. Although the term has different meanings in different jurisdictions and contexts, champions of open banking, including policymakers, industry representatives, and legal scholars, generally argue for more expansive data sharing between financial institutions and tech companies under the auspices of augmenting consumer control and competition between banks and tech companies.[1] According to this vision, banks, in particular, are jealously guarding deposits and consumer transaction data, hurting consumers, start-ups, and small businesses.[2] Open banking advocates argue financial institutions must allow customers to seamlessly move data and funds between accounts (often as quickly as possible).[3]

The financial technology—or "fintech"—companies in the open banking sector use consumer transaction data from financial institutions to develop applications for additional use cases, including deposit account switching, a credit card comparison shopping, personalized investment and wealth management, and lending based on analyses of cash flow, rent and utility bills, and other "alternative data" not typically collected by credit reporting agencies.[4] Familiar companies in the sector include lending platforms such as Rocket Mortgage and SoFi, investment platforms like Robinhood, and payment and stored-value platforms such as PayPal, Venmo, and Coinbase.

Many scholars argue fintech firms in this sector improve access to payment solutions and credit.[5] Policymakers and scholars tout open bank-

1. Consumer Fin. Prot. Bureau, Advance Notice of Proposed Rulemaking, Consumer Access to Financial Records, 85 Fed. Reg. 71003 (Nov. 6, 2020); Executive Order On Promoting Competition In The American Economy, Sec. 5(t), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy [https://perma.cc/LWE8-NHVR] (encouraging the CFPB to propose a rule concerning financial data sharing as part of a pan-executive agenda promoting competition). Some scholars and policymakers use the term "open finance" to include financial services beyond banking. I primarily use the term "open banking" in this Article to analyze banks and bank-like companies.

2. Dan Awrey & Joshua Macey, *The Promise & Perils of Open Finance*, 40 YALE J. ON REGUL. 1, 3-4 (2023).

3. A growing number of entities, including banks, now serve as both data providers and third parties. Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, 74797 (Oct. 31, 2023) [hereinafter Proposed Open Banking Rule].

4. *Id.* at 74798.

5. *See, e.g.*, Rory Van Loo, *Privacy Pretexts*, 108 CORNELL L. REV. 1, 54 (2022) (citing the CFPB 1033 Rule as regulation that could overcome pretexts of individual privacy harm that prevent financial data sharing); Cesare Fracassi & William Magnuson, *Data Autonomy*, 74 VAND. L. REV. 327, 328, 383 (2021) (offering a an expansive proposal for open banking); Rory Van Loo, *Making Innovation More Competitive: The Case of Fintech*, 65 UCLA L. REV. 232, 267 (2018) (critiquing the CFPB for stalling on open banking rules and pointing out that such rules

ing as offering new, more accessible, faster ways to pay people and new routes to credit and investment.[6] Although one must have a bank account to use most digital wallet features, per the same study, consumers opening digital wallet accounts tend to be less affluent than consumers opening accounts with the largest banks, such as Bank of America, Chase, Citi, and Wells Fargo.[7]

Yet, as most participants in the policy and academic debate acknowledge, open banking poses serious trade-offs compared to traditional banking and presents challenges for the future of financial services. In this Article, I address the challenges the current trajectory presents for consumer data governance.[8] Generally, I agree with supporters of open banking that existing reporting systems under-generate valuable data. Yet proponents are also underweighting the threats posed regarding the overgeneration of data.[9]

I focus on "digital wallets"—mobile smartphone applications primarily used for payments. According to an August 2023 survey, 53% of U.S. consumers prefer to use digital wallets rather than traditional payment methods.[10] For instance, Apple and Google offer "digital wallets" that store credit card information and other data so consumers can simply "tap to pay" at checkout.[11] However, I am concerned with companies like PayPal, Venmo, Cash App, and Coinbase, which offer wallets that store consumer balances outside the insured, regulated, and supervised bank-

are necessary for competition and innovation). For an analysis of CFPB Proposed Rule 1033 rooted in an autonomy view of privacy, generally arguing in favor of open banking, see Nikita Aggarwal, *Locating Consumer Credit Regulation*, CARDOZO L. REV. (forthcoming 2024) (also proposing a shift from focusing on limiting flows of consumer data, to enabling the secure flow of consumer data through product, conduct, and prudential regulation).

6. Proposed Open Banking Rule, *supra* note 3, at 74803, 74805, 74809 (highlighting "transaction-based underwriting" as a key "beneficial use case" of Open Banking). *See also, e.g.*, Marco Di Maggio & Dimuthu Ratnadiwakara, Invisible Primes: Fintech Lending with Alternative Data 9 n.10 (Jan. 8, 2024) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3937438 [https://perma.cc/N7W7-XNR3] (finding the fintech lender Upstart increased loan origination to previously marginalized high-risk, low credit score borrowers and credit invisibles).

7. More than half (52%) of consumers opening an account with a megabank in 2023 earn more than $75,000. Among new digital bank/fintech customers, just 21% earn that much. Ron Shevlin, *The Checking Account War is Over and the Fintechs Have Won*, FORBES (July 5, 2023). https://www.forbes.com/sites/ronshevlin/2023/07/05/the-checking-account-war-is-over-and-the-fintechs-have-won/?sh=3f0944f73a31 [https://perma.cc/ZW3S-Z539].

8. Data governance law is the "legal regime that regulates how data about people is collected, processed, and used." Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 573 (2021).

9. Peter Swire, *The Portability and Other Required Transfers Impact Assessment: Assessing Competition, Privacy, Cybersecurity, and Other Considerations*, 6 GEO. L. TECH. REV. 57, 57-58 (2022).

10. Amanda Claypool, *53% Of Americans Use Digital Wallets More Than Traditional Payment Methods: Poll*, FORBES (Aug. 25, 2023), https://www.forbes.com/advisor/banking/digital-wallets-payment-apps [https://perma.cc/9S8A-EUBQ].

11. *See, e.g.*, Ling Ling Ang, Will Taylor & Max Perez Leon, *Fintech Developments and Antitrust Considerations in Payments*, 35 AM. BAR ASS'N 69, 73 (2021).

ing system to enable faster and cheaper payments and money transfers.[12] According to one study, more than a third of Gen Zers and Millennials, and nearly three in ten Gen Xers, consider a digital wallet or banking app to be their primary checking account.[13]

The digital wallet sector emerged from Silicon Valley, not Wall Street. In 1999, a team including Peter Thiel (who later became a venture capitalist behind SpaceX, Airbnb, Yelp, LinkedIn, and Palantir) established a company called Confinity.[14] In 2000, Confinity merged with the original X.com, owned by Elon Musk (now the wealthiest person in the world, has gone on to found Tesla, SpaceX, and Neuralink and purchased Twitter, which he re-branded as the new X.com).[15] Thiel and Musk called their company PayPal, aiming to create "the world's first digital payment platform, making money work better, faster and easier than ever."[16] E-commerce giant eBay acquired PayPal in 2002 for $1.5 billion, cementing its position as the preferred payment option for online retail. In 2013, PayPal purchased Venmo, which college roommates Iqram Magdon-Ismail and Andrew Kortina had initially developed a prototype for sending payments through text messages before building an app.[17] Venmo has since emerged as the industry leader.

Cash App, a subsidiary of Block Finance, offers the second most-used digital wallet. Jack Dorsey, the founder of Twitter, founded Block in 2009, initially calling it Square.[18] The company developed a tablet-style point-of-sale system that we use at retail counters and restaurants today.[19] In 2013, a month following PayPal's acquisition of Venmo, Block

12. Roughly six in ten Americans who have ever used PayPal, Venmo, Zelle, or Cash App (61%) say a major reason for doing so is because it makes paying for things easier. About half of these users (47%) say a key factor for using these platforms is because it makes sending money to people safer. Smaller shares say a major reason they use these platforms is that other people they know use them (34%) or that it allows them to split expenses with others (21%). Monica Anderson, *Payment Apps Like Venmo And Cash App Bring Convenience – And Security Concerns – To Some Users*, PEW RSCH. CTR. (Sept. 8, 2022), https://www.pewresearch.org/short-reads/2022/09/08/payment-apps-like-venmo-and-cash-app-bring-convenience-and-security-concerns-to-some-users [https://perma.cc/EM84-C7VX].

13. *See* Shevlin, *supra* note 7.

14. Tami Brehse & Kylie Kirschner, *Members of the PayPal Mafia include tech titans like Elon Musk, Peter Thiel, and Reid Hoffman. Here's where they are now.*, BUS. INSIDER (Nov. 12, 2023, 4:40 AM EST), https://www.businessinsider.com/paypal-mafia-members-elon-musk-peter-thiel-reid-hoffman-companies [https://perma.cc/NE9B-2M33].

15. *Id.*

16. *History and Facts*, PAYPAL, https://about.pypl.com/who-we-are/history-and-facts/default.aspx [https://perma.cc/2QQY-BZH7].

17. Kendall Baker, *The Story of How Venmo Was Started*, THE HUSTLE (June 30, 2020), https://thehustle.co/story-venmo-started [https://perma.cc/8R5H-6GW2].

18. *About Square*, SQUARE (Nov. 2, 2009), https://squareup.com/us/en/about [https://perma.cc/8TPL-P5SW].

19. *Id.*

launched Square Cash, later rebranded Cash App.[20] Cash App is especially popular among Black, Hispanic, and low-income consumers.[21]

As many scholars have warned, some of the digital wallet companies evade banking laws.[22] Contrary to conventional wisdom, PayPal, Venmo, or Cash App balances are not nearly as safe for consumers as bank deposits. These companies issue private liabilities that are denominated in and pegged to fiat currency ($USD, etc.), but are only backed by other bank deposits and various bonds. Consumers lack standard bank account protections, including FDIC insurance in the event of the wallet company's failure. Over the past several years, many companies have developed wallets to hold cryptocurrency. For instance, Coinbase offers a combination payment and investment wallet, which can hold many cryptocurrencies, none of which are Coinbase liabilities.[23] Some coins, such as "stablecoins" issued by companies like Circle, Paxos, and Tether, present similar risks to PayPal, Venmo, and Cash App balances.[24] Banking regulators do not regularly examine or supervise the companies involved. Overall, the business practices of these companies undermine key goals of banking law: entry restriction, structural separation between banking and commerce, and financial stability.[25]

In this Article, I refer to the digital wallet balances, held out by technology companies as if they were as safe as FDIC-insured bank deposits, as "platform money." In part, I use this language to draw attention to the informational practices of the companies involved in the sector. I also use the term to highlight how technology companies are stacking data-intensive consumer applications "on top of" the U.S. banking system to profit from its deficiencies.

Legal scholars are increasingly analyzing the role of platforms and "platform power" in regulated industries, including finance, communications, transportation, energy, and finance.[26] Platform regulation is also a key feature of antitrust and competition law. In this Article, I engage with

20. *Square Cash Makes Sending Money as Easy as Sending an Email*, SQUARE, https://squareup.com/us/en/press/square-cash-makes-sending-money-as-easy-as-sending-an-email [https://perma.cc/R5LZ-TSZ9].

21. *See* Anderson, *supra* note 12.

22. *See generally* Nadav Orian Peer, *Money Creation and Bank Clearing*, 28 FORDHAM J. CORP. & FIN. L. 35 (2023); Dan Awrey, *Bad Money*, 106 CORNELL L. REV. 1 (2020); Dan Awrey & Kristin van Zwieten, *The Shadow Payment System*, 43 J. CORP. L. 775 (2018).

23. *Coinbase User Agreement*, COINBASE, https://www.coinbase.com/legal/user_agreement/united_states [https://perma.cc/EP7D-CGEX].

24. *See infra* Part II.

25. *See generally* Todd Phillips & Matthew Adam Bruckner, *Consumer Shadow Banks*, 35 STAN. L. & POL'Y REV. 226 (2024); Arthur E. Wilmarth, Jr., *We Must Protect Investors and Our Banking System from the Crypto Industry*, 101 WASH. U. L. REV. 235, 320 (2023) (arguing that Congress should prohibit entities that are not FDIC-insured banks from offering any type of shadow deposits (short-term financial claims that function as de facto deposits)).

26. *See infra* Part II.

these perspectives but primarily draw on the concepts of platform power used in the emerging legal literature on information platforms. Insights from this literature help us trace the network effects of data governance, re-envision power within business ecosystems, and suggest regulatory alternatives.

In particular, I focus on the role of data brokers in the "platform money" ecosystem. By transferring credentials and account information between apps, data brokers provide the critical infrastructure of open banking. However, like Amazon, Google, and Meta, they serve multiple businesses and consumers.[27] For instance, data brokers often claim they merely provide "the pipes" between banks and fintech companies.[28]

But in a platform economy, to control "pipes" between the finance and technology sectors is to exercise enormous legal, political, and economic power. For instance, when transferring balances, the dominant financial data broker, Plaid gives both Plaid and its partners access to a user's identity information, including name, address, email, and phone number; entire transaction and balance history, including a geolocation and category for each purchase made. Plaid can share additional data regarding consumer debt, savings, public benefits receipt, tax payments, property, investments, and other data it reserves the right to use. While providing a generic service, the brokers collect, use, and retain more data than necessary to transfer funds, to use for their own purposes.

Like most other financial technology (fintech) companies, brokers tend toward *"data maximization"*—toward perpetually sharing data and amplifying information under the premise it will necessarily improve desired outcomes.[29] This is not to say that different companies do not treat data differently, but to various degrees, they analyze transaction data to reconstitute people into "data doubles," which can then be sorted, stored, scored, shared, and sold.[30] While analyzing data, they may also apply machine learning and other advanced analytics to generate valuable insights about consumer behavior, preferences, and creditworthiness, which they can then use these insights to improve the design, marketing, and algo-

27. *See* Awrey & Macey, *supra* note 2, at 5-6 ("[D]ata aggregation thus bears all the hallmarks of a 'two-sided market' in which strong network effects on each side of the market serve to attract users on the other side.").

28. Letter from Chi Chi Wu, Nat'l Consumer Law Ctr., to Kathleen Kraninger, Director, Consumer Fin. Prot. Bureau 8 (Feb. 12, 2020), https://www.nclc.org/wp-content/uploads/2022/08/NCLC-statement-for-CFPB-1033-Symposium-1.pdf [https://perma.cc/SD2P-SGMC]. *See also* Alex Konrad, *Fintech's Happy Plumbers*, FORBES, https://www.forbes.com/plaid-fintech/#581f894267f9 [https://perma.cc/CBY8-6QLU].

29. *See, e.g.*, Omri Ben-Shahar, *Data Pollution*, 11 J. LEGAL ANALYSIS 104, 140 (2019).

30. For a deeper discussion of these processes, see, for example, JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 63-74 (2019).

rithmic pricing.[31] Fintech companies and their partners claim that mass data collection makes financial services faster and easier, but also more automated, sophisticated, objective, predictive, accurate, and neutral, yielding more comprehensive assessments of human behavior.[32]

I have contributed to an emerging literature on digital privacy and data governance championing *data minimization*—the restriction of data collection, processing, storage, and sharing to avoid unnecessary risks and costs.[33] In a previous work, I have analyzed the chronic, social harms of overcollection of financial data and how it affects how we participate, associate, and build economic relationships.[34] I argue privacy is vital for informed citizenship, public debate, innovation, and democracy itself.[35] Government agencies, including law enforcement agencies, abuse financial data collected by companies, as I have surveyed in the context of public benefits disqualification, immigration enforcement, the criminalization of reproductive health services, and re-entry and parole[36] In general, data maximization exacerbates the security and privacy risks of financial services, including the risk of theft of funds and identity.[37] For example, as this Article goes to print, customers of online lenders like Juno, Yieldstreet, and Yotta are still attempting to recover funds and manage downstream harms after the operational and financial collapse of Synapse, a "banking-as-a-service" (BaaS) intermediary.[38]

But the platform money business also poses acute, specific consumer harms. According to Pew Research, about 10% of fintech payment users (and 20% of low-income users) say they have fallen victim to scams or

31. *See, e.g.*, ERIC A. POSNER & E. GLEN WEYL, RADICAL MARKETS: UPROOTING CAPITALISM AND DEMOCRACY FOR A JUST SOCIETY 208-09 (2018).

32. *See, e.g.*, FRANK PASQUALE, THE NEW LAWS OF ROBOTICS 119-24, 131-36 (2019).

33. *See, e.g.*, Mireille Hildebrandt, *Primitives of Legal Protection in the Era of Data-Driven Platforms*, 2 GEO. L. TECH. REV. 252, 267 (2018) (also arguing minimization improves the methodological integrity of algorithms). The International Fair Information Practice Principles (FIPPs), a framework guiding government and industry data practices, contains a thinner definition of data minimization, situating limitations within outdated consent theories. *Fair Information Practice Principles*, FTC (June 25, 2007), https://web.archive.org/web/20090331134113/http://www.ftc.gov/reports/privacy3/fairinfo.shtm [https://perma.cc/FP82-57N9]. The GDPR also relies on the concept. *See infra* Part I.

34. *See generally* Raúl Carrillo, *Seeing Through Money: Democracy, Data Governance, and the Digital Dollar*, 57 GA. L. REV. 1207 (2023).

35. *Id.* at 1233.

36. *See generally id.*

37. *See, e.g.*, Cheng-Yun Tsang, *From Industry Sandbox to Supervisory Control Box: Rethinking the Role of Regulators in the Era of Fintech*, 2019 U. ILL. J.L. TECH. & POL'Y 355, 373 ("data sharing activities subject data owners and customers to increasing cyber and privacy risks and begs the question of how liability among all parties in a sharing arrangement should be reasonably allocated").

38. Rob Copeland, *What Happens When Your Bank Isn't Really a Bank and Your Money Disappears?*, N.Y. TIMES (July 11, 2024), https://www.nytimes.com/2024/07/09/business/synapse-bankruptcy-fintech-fdic-insurance.html [https://perma.cc/2P8A-R99P]

hacking, leading to loss of funds.[39] (Generally, a hacker is more likely to compromise a digital wallet than a bank account app because the data is richer and less protected).[40] Consumers do not have the right to manage information generated by their transactions or correct how brokers score data, even if the scoring is discriminatory.[41] Remedies for informational harms (at best, minor litigation damages) are typically limited, foreclosing the possibility that customers obtain sufficient compensation for injury from collectors.[42] Most critically, breaches increase the likelihood of the composite harm of identity theft or "identity fraud" (the appropriation and use of someone else's identity).[43]

Nizan Gaslevich Packin has argued that consumers should have the legal right to manage their financial data as they see fit, but the CFPB should regulate "data aggregators" according to principles like transparency, informed consent to data sharing, and promotion of competition, mirroring Australian open banking law.[44] The CFPB has incorporated many of these principles into its Proposed Open Banking Rule. Dan Awrey and Josh Macey have explored the economics of data aggregation, arguing that to prevent "market concentration, the abuse of monopoly power, and the creation of a new breed of too-big-to-fail institutions," Congress should pass new legislation that would impose a licensing regime for data aggregators, the development of standardized, interoperable infrastructure, universal access to data for businesses and consumers, and structural separation of data aggregation from finance.[45]

In this Article, I explore the distinct challenges financial data brokers present within the platform money ecosystem from a consumer financial protection perspective. I synthesize concerns regarding banking law and data governance, shedding light on the intricate web of issues and underscoring the urgent need for regulatory measures to address these challenges. While doing so, I recontextualize the role of competition, in large part because the CFPB lacks an overarching statutory mandate to promote competition.

Adopting this critical perspective, I argue that when data brokers collect, use, and retain data from balance transfers for their secondary purposes, the broker's profits from banking law arbitrage and risk violating federal consumer financial protection law. Consumers hardly know

39. *See* Anderson, *supra* note 12.

40. Carrillo, *supra* note 34, at 1259.

41. *Id.*

42. *Id.*

43. *Identity Theft*, U.S. DEP'T OF. JUST. (June 9, 2015), https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud [https://perma.cc/5L7G-DTQT].

44. *See generally* Nizan Geslevich Packin, *Show Me the (Data About the) Money!*, 2020 UTAH L. REV. 1277 (2020).

45. Awrey & Macey, *supra* note 2, at 7 ("so that the forces of competition continue to drive innovation and push the boundaries of this frontier tomorrow and beyond.").

the existence of data brokers, much less how they use data. Even brokers do not know the eventual destination or use of the data, meaning consumers cannot meaningfully consent to data brokers' business practices. Accordingly, the CFPB should prevent data brokers transferring funds between bank accounts and digital wallets like PayPal, Venmo, Cash App, and Coinbase from collecting, using, or retaining more data than is strictly necessary to transfer those funds in compliance with existing laws (such as laws against fraud, money laundering, and terrorism financing).

My proposal would preserve consumers' ability to transfer funds and switch accounts while effectively ending the data mining of simple balance transfers. The rule would also have positive and negative knock-on effects on other components of the open banking sector. Regardless, a robust data minimization standard is critical in protecting consumers from the emergent threats of data maximization in a new generation of consumer banking. The proposal is also a crucial step toward a "regulated industries" approach in consumer finance, promoting a continuum of public governance over critical networks, platforms, and utilities rather than competition per se.

In Part II, I map the world of platform money and expand on how fintech companies evade banking regulation. The FDIC, OCC, and Fed lack the authority to designate a nonbank company as a bank, meaning platform money issuers escape appropriate insurance, leverage, capital, and liquidity requirements, among other issues. The companies also pool customer balances, place them in chartered banks, and can withdraw them from the banks at any time, triggering concerns regarding deposit flight and volatility.

In Part III, I discuss the core role of data brokers in the platform sector. The unaccountable brokers exacerbate the security and privacy risks of simple balance transfers, including the risk of theft of funds and identity, far beyond the status quo. Yet financial data governance laws, including the Fair Credit Reporting Act (FCRA), are so antiquated and weak that they do not sufficiently govern how traditional financial services companies, much less data brokers, sort, store, score, and share our data. Consumer advocates argue the business ecosystem is increasingly susceptible to fraud and has already harmed consumers.

In Part IV, I critique existing policymaking approaches to platform money. Recently, the CFPB laudably proposed an Open Banking Rule, which should help consumers locked into bad relationships with their banks and establish guardrails for potentially beneficial practices. However, in advocating for consumers to be able to move funds as quickly and freely as possible, the Bureau is also prioritizing competition between fintech companies and banks in ways that exacerbate structural problems banking regulators cannot address. Moreover, it establishes an insufficient data minimization standard, hinging on outdated individualized,

consent-based privacy law standards, limiting data collection, use, and retention to what is "reasonably necessary" to provide services.

In Part V, I argue that the business practices of brokers in the Platform Money ecosystem unduly threaten harm to consumers. I propose an amendment to the Open Banking Rule: the CFPB should pivot and declare that when transferring balances between FDIC-insured depository institutions and certain digital wallets (stored value accounts per the CFPB),[46] it is an unfair, deceptive, and abusive practice for a data broker (a 'data aggregator' per the CFPB)[47] to collect, use, or retain more data than is strictly necessary to transfer a balance and comply with existing laws" (e.g. anti-money laundering laws).[48]

Collecting, using, or retaining more data than necessary in this context is an unfair practice. The volume and volatility of data are likely to risk widespread consumer harm. Even the rare consumer who knows data brokers that mine transfer data cannot meaningfully consent to data collection because of the nature of open-ended data-sharing practices. They cannot reject brokers' services if they want to use platform money. While digital wallets may benefit consumers and competition, the brokers' data siphoning enriches the data brokers while hurting consumers. The practices are deceptive because brokers take advantage of reasonable consumer assumptions that brokers merely help transfer funds, not collect, and share data like Meta, Amazon, or Google. The practices are abusive because brokers take unreasonable advantage of (1) a lack of consumer understanding regarding the risks of platform money, (2) the inability of consumers to select a broker, much less protect their interests against that broker, and (3) the reasonable reliance of the consumer that data brokers act in their interest.

---

46. In its official regulations, due to the legacy of terms used in the EFTA, the Bureau refers to digital wallets account holding funds as stored value accounts. The term refers to the types of platform money I discuss in this Article, but also includes, for instance, some prepaid debit cards, which also hold deposit-equivalents. *See, e.g.*, *Analysis of Deposit Insurance Coverage on Funds Stored Through Payment Apps*, CFPB (June 1, 2023), https://www.consumerfinance.gov/data-research/research-reports/issue-spotlight-analysis-of-deposit-insurance-coverage-on-funds-stored-through-payment-apps/full-report [https://perma.cc/F6B9-VF3Y].

47. The CFPB defines a "data aggregator" (which I refer to as data brokers) as an entity that is retained by and provides services to the authorized third party to enable access to covered data. Proposed Open Banking Rule, *supra* note 3, at 74807. Other jurisdictions distinguish between brokers and aggregators. In California, "data broker" refers to a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. In Vermont, a "data broker" is a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship. As I do not place much import on the distinction between selling and sharing data, I do not emphasize the difference in nomenclature.

48. Emma C. Jordan, *The Hidden Structures of Inequality: The Federal Reserve and a Cascade Of Failures*, 2 U. PA. J. L. & PUB. AFFAIRS (2017).

In Part VI, I argue my proposed amendment to the Open Banking Rule is a critical initial step in exercising public governance over the future of consumer banking. We should regulate private sector technology built on top of the banking system with due sensitivity. My proposal promotes three common goals for governing networks, platforms, and utilities by (1) establishing public obligations for general access and service, (2) increasing structural separation between banking and commerce, and (3) encouraging the use of new "public fintech" infrastructure, including the Fed's new platform for instantaneous bank transfers, which would minimize the use cases for platform money.

II. Platform Money

In a new casebook on "networks, platforms, and utilities," Morgan Ricks, Ganesh Sitaraman, Shelley Whelton, and Lev Menand adopt a broad definition of platforms as "large-scale, centralized places—physical or virtual—that allow people to interact or transact."[49] As examples, they cite 19th-century stockyards, grainhouses, and railroads, as well as contemporary stock exchanges, online stores, and social media companies.[50] Sabeel Rahman has adopted a similarly broad vision, characterizing online platforms as "linking producers and consumers of goods, services, and information."[51]

In 2003, economists Jean Tirole and Jean-Charles Rochet proffered a theory of platforms as two-sided markets, characterizing "markets with network externalities."[52] Common platforms draw a wide range and critical mass of buyers and sellers. Benefits to buyers and sellers ultimately depend upon the platform. Companies may operate a platform but also market their own goods and services on that platform, entrenching dominance, thwarting competition, and stifling innovation.[53]

Technology companies have created "payment platforms," connecting buyers and sellers of goods and services, but controlling the terms of those connections.[54] Most U.S. consumers trust apps at least as much as

49. *See* MORGAN RICKS, GANESH SITARAMAN, SHELLEY WELTON & LEV MENAND, NETWORKS, PLATFORMS, AND UTILITIES: LAW AND POLICY 7 (2022).

50. *Id.*

51. K. Sabeel Rahman, *The New Utilities: Private Power, Social Infrastructure, and the Revival of the Public Utility Concept*, 39 CARDOZO L. REV. 1621, 1668-69 (2018).

52. *See generally* Jean-Charles Rochet & Jean Tirole, *Two-Sided Markets: A Progress Report*, 37 RAND J. ECON. 645 (2006); Jean-Charles Rochet & Jean Tirole, *Platform Competition in Two-Sided Markets*, 1 J. EUR. ECON. ASS'N 990 (2003) (explaining the dynamics of competition in two-sided markets).

53. Lina M. Khan, *The Separation of Platforms and Commerce*, 119 COLUM. L. REV. 973, 976-77 (2019).

54. *See, e.g.,* Dan Awrey, *Unbundling Banking, Money, and Payments*, 110 GEO. L.J. 715, 719 (2022); Dan Awrey & Kristin van Zwieten, *The Shadow Payment System*, 43 J. CORP. L. 775, 816 (2018) (discussing 'shadow payment platforms').

they trust debit and credit card payments.[55] Consumers can download platform money apps and use most features for free. Once a consumer connects an app like PayPal, Venmo, Cash App, or Coinbase Wallet to a debit card, credit card, or bank account and imports funds, they can send money from the app to a friend's or family member's app. Like most technology companies, they constantly seek a more expansive user base.[56] Indeed, Venmo arguably became so popular because of its social media features, including a "global social media" feed detailing payments by people around the world until 2021.[57] According to recent statistics, three-quarters of U.S. adults have used payment apps, and volume hit nearly $1.1 trillion in 2022,[58] quadrupling since 2018.[59]As the apps are free for consumers, they are only likely to become more popular. Although the wallet companies charge merchants to use the app,[60] they are cheaper to use than conventional merchant banking services enabling debit or credit card payments.[61]

However, consumers and businesses do not just make payments with these apps. They also store funds in their wallets (potentially indefinitely). The CFPB estimates that U.S. consumers have stored billions of dollars on nonbank payment apps.[62] Although conventional wisdom maintains that digital wallet balances are small, policymakers and the public

55. Erin El Issa, *Most Americans Go Mobile With Payment Apps—Here's How They Roll*, NERDWALLET (Feb. 26, 2020), https://www.nerdwallet.com/article/banking/mobile-payment-app-survey [https://perma.cc/L7GR-RFZ5].

56. *See, e.g.*, BANK FOR INT'L SETTLEMENTS (BIS), ANNUAL ECONOMIC REPORT 56 (2019), https://www.bis.org/publ/arpdf/ar2019e3.htm [https://perma.cc/8WVT-E9AW] (discussing Big Tech's involvement with financial services). For instance, Venmo does not charge individual users for sending or receiving payments, nor does the company charge any monthly or annual fees. However, Venmo transfers may take a few days. Venmo apps charge fees, usually 25 cents, for faster access. Venmo generates revenue via its interchange and withdrawal fees, interest on cash, and fees for cashing checks, Pay With Venmo, and affiliate commissions on its cashback program. Venmo also charges a 3% fee it charges for credit card transactions. Julius Mansa, *Venmo: Its Business Model and Competition*, INVESTOPEDIA (Feb. 10, 2022), https://www.investopedia.com/articles/personal-finance/010715/venmo-its-business-model-and-competition.asp [https://perma.cc/JGD2-2R7T]. It also offers unique credit cards (such as its Venmo-branded Synchrony Bank card) or card payments with a merchant fee. Kate Rooney, PayPal is launching a Venmo credit card to help monetize the payment app, CNBC (Oct. 17, 2019), https://www.cnbc.com/2019/10/17/paypals-venmo-is-launching-a-credit-card.html [https://perma.cc/4GAC-EKGE].

57. Ian Carlos Campbell, *Venmo drops the global social feed that could make your payments visible to strangers*, THE VERGE (July 20, 2021), https://www.theverge.com/2021/7/20/22585467/venmo-removes-global-social-feed-private-payments [https://perma.cc/32DZ-96QC].

58. Anderson, *supra* note 12.

59. CFPB, *Issue Spotlight: Analysis of Deposit Insurance Coverage on Funds Stored Through Payment Apps*, at n.1, https://www.consumerfinance.gov/data-research/research-reports/issue-spotlight-analysis-of-deposit-insurance-coverage-on-funds-stored-through-payment-apps/full-report [https://perma.cc/867B-YQMC] [hereinafter CFPB Issue Spotlight].

60. Awrey, *supra* note 22, at 41.

61. *Id.*

62. *See* CFPB Deposit Spotlight, *supra* note 59.

lack sufficient data regarding average or median balances.[63] According to one 2021 report, Cash App reportedly held roughly $40 per customer on average as of the end of Q2 2021, while PayPal held approximately $77 per active account.[64] However, it is unclear that this dataset removes zero-account balances or rarely used accounts, providing a more meaningful assessment of consumer impacts. Moreover, these figures do not capture the dynamics of balance transfers.

On average, users keep up to $287 in their account before transferring it to their bank account, with 46% of app users keeping over $100 in their account.[65] Gen Xers and millennials keep more money in their accounts than other generations ($405 and $337, respectively, versus $88 for Gen Zers and $189 for Baby Boomers, on average).[66]

In any case, platform money companies and their business partners increasingly profit from keeping customer funds in the apps and out of the regulated banking system. Scholars have argued that from the perspective of consumer banking regulation, platform money is unsafe.[67] The FDIC does not insure most of these balances, and consumers lack standard bank account protections.[68]

Most companies commingle funds, depositing customer funds in banks in the company's name (essentially providing the customer with an IOU). Some invest customer balances in interest-earning funds but do not share returns with consumers. They also charge consumers for enhanced wallet features (e.g., faster transfers or links to pre-paid debit or credit card accounts). Some platform money companies sell prepaid debit cards, partner with tech companies to offer tech-company-branded credit cards or supply international remittance services.[69]

63. Unlike banks, wallet companies do not have to provide regulators with detailed information regarding their liabilities to consumers. However, to the extent a nonbank payment company is a public company, it must also comply with relevant federal and state securities laws, including certain financial disclosures.

64. U.S. DEP'T OF THE TREASURY REP. TO THE WHITE HOUSE COMPETITION COUNCIL, ASSESSING THE IMPACT OF NEW ENTRANT NON-BANK FIRMS ON COMPETITION IN CONSUMER FINANCE MARKETS 62 n.263 (2022), https://home.treasury.gov/system/files/136/Assessing-the-Impact-of-New-Entrant-Nonbank-Firms.pdf [https://perma.cc/H7S7-K8V6].

65. Issa, *supra* note 55.

66. *Id.*

67. *See, e.g.*, Phillips & Bruckner, *supra* note 25; Wilmarth, *supra* note 25.

68. For the most part, PayPal, Venmo, Cash App, and the other wallet providers discussed in this Article do not offer FDIC-insured accounts. However, some "neobanks" do offer insurance via partnership. For instance, the Chime app is a digital interface for consumers, but Chime's partnering banks, The Bancorp Bank and Stride Bank, hold Chime consumer funds in accounts in the consumers' names. Carson Kessler, *A Banking App Has Been Suddenly Closing Accounts, Sometimes Not Returning Customers' Money*, PROPUBLICA (July 6, 2021), https://www.propublica.org/article/chime [https://perma.cc/DWF7-HCFA].

69. *See* CFPB Proposes New Federal Oversight of Big Tech Companies and Other Providers of Digital Wallets and Payment Apps, CFPB (Nov. 7, 2023), https://www.consumerfinance.gov/rules-policy/rules-under-development/defining-larger-participants-of-a-market-for-general-use-digital-consumer-payment-applications [https://perma.cc/J3UR-5Y66] This may also

Users increasingly use digit wallet accounts to store cryptocurrency, which they can trade or use for payments within the same app. Of particular relevance, "stablecoin" issuers promise their products are pegged to the dollar 1:1 and as stable as bank deposits. For instance, in consortium with other cryptocurrency companies, including members of Coinbase, Circle issues a 'stablecoin'[70] called the U.S. Dollar Coin (USDC).[71] Circle markets USDC as a "Digital Dollar," implying it is just as valuable and reliable as government money—as stable as the dollar bill in your pocket.[72] However, much like a PayPal, Venmo, or Cash App balance, USDC is a privately issued liability, merely denominated or pegged to fiat currency ($USD, etc.), backed by bank deposits and various bonds.[73] The Digital Dollars in a Coinbase wallet are not, legally speaking, anything like a U.S. dollar bill.

A. Technology at the Banking Perimeter

Many policymakers, scholars, and banking industry representatives have expressed concern about how platform money issuers assume banking rights without the corollary responsibilities. Banks are unique legal entities within our monetary system. It is much more challenging for companies to obtain banking charters than the average corporate charter.[74] I have joined other scholars in treating banks as public utilities, infrastructure, franchises, or similar institutions.[75]

---

link consumers to riskier financial services and products—for instance, "buy now, pay later" (BNPL) loans or "earned wage access" products. *See, e.g.*, Nakita Q. Cuttino, *The Rise of "FringeTech": Regulatory Risks in Earned-Wage Access*, 115 NW. U. L. REV. 1505 (2021).

70. *Introducing USDC: Earn 5.1% rewards by simply holding USDC on Coinbase*, COINBASE, https://www.coinbase.com/usdc [https://perma.cc/KXT8-VCCV].

71. Ian Allison, *Coinbase Gets a Stake in Stablecoin Operator Circle and USDC Adds 6 New Blockchains*, COINDESK (Aug. 21, 2023), https://www.coindesk.com/business/2023/08/21/coinbase-buys-a-stake-in-stablecoin-operator-circle-and-usdc-adds-6-new-blockchains [https://perma.cc/99V8-JU64]; Ana Alexandre, *Coinbase and Circle Launch USDC Stablecoin With Purported Full Backing in US Dollars*, COINTELEGRAPH (Oct. 24, 2018), https://cointelegraph.com/news/coinbase-and-circle-launch-usdc-stablecoin-with-purported-full-backing-in-us-dollars [https://perma.cc/J9KA-VYMK].

72. I borrow my definition from the STABLE Act, which I co-drafted along with my colleague Rohan Grey. The STABLE Act proposes to regulate stablecoins as bank deposits. *See* Stablecoin Classification and Regulation Act of 2020 (STABLE) Act, Discussion Draft, 116th Cong. § 2 8-11 (2020) (introduced by Rep. Rashida Tlaib). *See also* Wilmarth, *supra* note 25, at 312-13 (also arguing that Congress should require all issuers and distributors of stablecoins to be FDIC-insured banks).

73. Joe Light & Vildrana Hajric, *Coinbase, Circle Say USDC Reserves to be in cash, treasuries*, BLOOMBERG LAW (Aug. 23, 2020), https://www.bloomberg.com/news/articles/2021-08-23/coinbase-circle-to-move-all-usdc-reserves-into-cash-treasuries [https://perma.cc/GU9F-7358].

74. Lev Menand, *Why Supervise Banks? The Foundations of the American Monetary Settlement*, 74 VAND. L. REV. 951, 958 (2021).

75. *See generally, e.g.*, Carrillo, *supra* note 34; Lev Menand & Morgan Ricks, *Rebuilding Banking Law: Banks as Public Utilities*, 41 YALE J. ON REGUL. 591; Mehrsa Baradaran, *Banking on Democracy*, 98 WASH. U. L. REV. 353, 358 (2020); Rohan Grey, *Administering Money: Coinage, Debt Crises, and the Future of Fiscal Policy*, 109 KY. L.J. 229 (2020); Rahman, *supra* note 51,

Most importantly, for our purposes, the federal government empowers banks to "create money" we use in our economy.[76] When a bank creates a loan and credits a customer account—"making a deposit"—or accepts payment of outside funds—"taking a deposit"—the deposit money is just as good as the dollar in your pocket." This promise is a special claim, as it implies the backing and "full faith and credit" of the U.S. government. The law reserves the claim for banks, who accept a specific set of responsibilities and rights. Other actors in the financial system benefit from the stabilizing role of banks in creating new markets, activities, and products.[77]

Federal and state-chartered banks receive access to the Federal Reserve discount (emergency backstop) window, Fed payment services, and FDIC deposit insurance (up to $250,000 per depositor per account).[78] In turn, regulators subject banks to prudential ("safety and soundness") regulations—including capital and liquidity requirements[79]—and ongoing examinations that impact their business models. One federal banking regulator (the FDIC, OCC, or Fed) supervises each bank, with numerous objectives, including reducing the probability and severity of runs and system-wide failures. In the event of collapse, the FDIC subjects banks to a unique resolution process rather than the general corporate bankruptcy process.[80]

When a company suggests that platform money is just as safe as a bank deposit—a legally protected instrument category—it is breaching the banking perimeter, in banking law parlance.[81] However, banking reg-

Robert C. Hockett & Saule T. Omarova, *The Finance Franchise*, 102 CORNELL L. REV. 1143 (2017); ARTHUR E. WILMARTH, TAMING THE MEGABANKS: WHY WE NEED A NEW GLASS-STEAGALL ACT (2020); Alan M. White, *Banks as Utilities*, 90 TULANE L. REV. 1241 (2016); Morgan Ricks, *Money as Infrastructure*, 2018 COLUM. BUS. L. REV. 757 (2018); Mehrsa Baradaran, *Banking and the Social Contract*, 89 NOTRE DAME L. REV. 1283 (2014). *See also* Stephanie Kelton & Paul McCulley, *The Fed Chair Should Be a Principled Populist*, N.Y. TIMES (Oct. 30, 2017) ("Banks are many things, but at their core, they have a public utility function . . . In that sense, banks are not different from the gas company or the electric company, connecting you to the grid.").

76. United States v. Philadelphia Nat'l Bank, 374 U.S. 321, 326 (1963). *See also* Brief of Thirty-Three Banking Law Scholars as *Amici Curiae* in Support of Appellee, Lacewell v. OCC (2020) (concerning the OCC's proposal for a "special fintech charter").

77. *See generally*, Saule T. Omarova, *New Tech v. New Deal: Fintech as a Systemic Phenomenon*, 36 YALE J. ON REGUL. 735 (2019).

78. Depositors may spread deposits among multiple institutions, placing $250,000 in each account. So long as depositors adopt this strategy, the federal government protects their money from bank failure. *See* 12 U.S.C. § 1821.

79. *See, e.g.*, 12 C.F.R. § 3.1 *et seq*. (providing capital standards for national banks).

80. Scholars and policymakers have excluded banks from bankruptcy by citing the differences between banks and other corporations. Matthew Bruckner, *Who's Down with OCC('s Definition of "Banks")?*, 24 U. PA. J. BUS. L. 144, 147-48 (2021).

81. *See, e.g.*, Nicholas K. Tabor, Katherine E. Di Lucido & Jeffery Y. Zhang, *A Brief History of the U.S. Regulatory Perimeter* 29 (Fed. Rsrv. Bd., Fin. & Econ. Discussion Series 2021-051, 2021), https://www.federalreserve.gov/econres/feds/files/2021051pap.pdf [https://perma.cc/PNV2-U8ME].

ulators have struggled to prevent non-bank companies from making this promise due to idiosyncratic statutory definitions, wayward regulatory interpretation, and doctrinal maldevelopment. The Banking Act of 1933, a response to the Great Depression, established the FDIC.[82] Four provisions of this statute, colloquially referred to as the Glass-Steagall Act, separated banking and commercial activities. Although the GLBA repealed provisions, two sections of the Glass-Steagall Act remain in effect.[83] Section 21 prohibits a company without a banking charter from holding consumer deposits.[84] Indeed, some experts have argued that it is a criminal offense for nonbanks to hold deposits.[85]

Unfortunately, the Glass-Steagall Act does not define "deposit," meaning regulators cannot easily invoke Section 21 against non-banks offering deposit-like products. Even if regulators or courts were to attempt to borrow the definition of "deposit" from another statute, there would be "no practical way forward."[86] For instance, the FDIA defines a "deposit" as "money or its equivalent received or held by a *bank*."[87] Yet federal laws contain several different laws and potentially conflicting definitions of a "bank."[88] For instance, the Banking Act of 1933 classifies "banks" as institutions that take "deposits" chartered, examined, and regulated by state or federal banking authorities.[89] Thus, the recursive definitions of "deposit" and "bank" create a "perfect legal circle."[90]

Overall, there is widespread acknowledgment that the current regulatory perimeter arguably restricts the activities of regulated banks but struggles to keep non-bank corporations from engaging in bank-like activity without bank-like regulation and supervision).[91] Non-banks issue deposit-like liabilities with relative impunity. Congress has not managed

82. The statutory provisions creating the FDIC in 1933 were codified as Section 12B of the Federal Reserve Act. Banking Act of 1933, Pub. L. No. 73-66, § 8, 48 Stat. 168 (codified as amended at 12 U.S.C. § 261, 262, 342 (2006)).

83. John Crawford, *A Better Way to Revive Glass-Steagall*, 70 STAN. L. REV. ONLINE 1, 2 (2017).

84. *See* 12 U.S.C. § 378(a)(2). For a broader interpretation of this statute within banking law informing this Article, see generally Wilmarth, *supra* note 25, and Morgan Ricks, *Entry Restriction, Shadow Banking, and the Structure of Monetary Institutions*, 2 J. FIN. REGUL. 291 (2016).

85. *See, e.g.*, Federalist Society, *Financial Regulation: The Apotheosis of the Administrative State*, 25 CONN. INS. L. J. 1, 8 (2018); Arthur E. Wilmarth, Jr., *The Road to Repeal of the Glass-Steagall Act*, 17 WAKE FOREST J. BUS. & INTELL. PROP. L. 441, 459-60 (2017).

86. Ricks, *supra* note 75, at 812.

87. 12 U.S.C. § 1813(l) (emphasis added).

88. For discussions of these definitions, see, for example, Dan Awrey & Kristin van Zwieten, *The Shadow Payment System*, 43 J. CORP. L. 775, 816 (2018); Saule T. Omarova & Margaret E. Tahyar, *That Which We Call A Bank: Revisiting the History of Bank Holding Company Regulation in the United States*, 31 REV. BANKING & FIN. L. 113, 115 (2011).

89. 12 U.S.C. § 1841(c)(1)(B).

90. *See* Ricks, *supra* note 75, at 812.

91. *See generally* Tabor et al., *supra* note 81.

to solidify banking law.[92] Banking regulators could attempt to promulgate rules clarifying the definitions of "bank" and "deposit," but courts have generally been unwilling to expand the scope of such statutory terms.[93]

Thus, platform money companies issue consumer bank-like promises but cannot keep those premises in the event of distress. Platform money companies could suffer classic runs,[94] along the same lines as Silicon Valley Bank and consumers would have minimal recourse for loss of funds.[95] Some companies also commingle consumer funds and place them in regulated banks, exposing them to deposit flight.[96] Indeed, during the run on Silicon Valley Bank, Circle, which held uninsured deposits at the bank, nearly collapsed.[97] It could only honor its promise to consumers because the Fed made all uninsured SVB depositors whole.

In some specific instances, platform money issuers offer consumers a restricted, incomplete version of FDIC insurance, known as 'pass-through insurance."[98] In a 'pass-through insurance' arrangement, "agents, nominees, custodians, and brokers" may establish an FDIC-insured deposit

92. *See generally id.* (arguing that while the current regulatory perimeter restricts the activities of regulated banks, it struggles to keep non-bank corporations from engaging in bank-like activity without bank-like regulation and supervision).

93. For instance, in *Board of Governors v. Dimension Financial Corp*, 474 U.S. 361, 374 (1986), the Court struck down a Board regulation intended to expand the Bank Holding Company Act (BHCA) definition of "bank" to cover "nonbank banks."

94. Rory Van Loo, *Digital Market Perfection*, 117 MICH. L. REV. 815, 820-21 (2019) (arguing AI could create a new type of bank run if they were to direct millions of consumers to switch banks). *See also* Hilary J. Allen, *Payments Failure*, 62 B.C. L. REV. 453, 454 (2021) (raising the possibility of a financial crisis precipitated by operational failures, more akin to a rolling blackout than a bank run).

95. They would not be allowed to make consumers whole until it had made shareholders and other creditors whole first. Unless the Fed bailed out the companies or organized a private-sector bailout. The Fed has questionable legal authority over companies operating beyond the banking perimeter unless it were to claim these companies are systemically important to the financial system.

96. For a standard Venmo Account, Venmo combines most customer funds and invests them per state money transmitter laws. Venmo is entitled to all returns on investment. Venmo places some funds in partner banks (currently Bancorp Bank, Goldman Sachs, and Wells Fargo). *See Holding Money in Your Venmo Account*, VENMO (Mar. 27, 2024), https://venmo.com/legal/us-user-agreement [https://perma.cc/6EK3-V4QU] [hereinafter *Venmo User Agreement*]. For Cash App Balance accounts, Cash App combines consumer funds in "pooled bank accounts" in Cash App's name. See *Cash App Terms of Service*, CASH APP (Apr. 4, 2024), https://cash.app/legal/us/en-us/tos#cash-account [https://perma.cc/7KVK-54MN] [hereinafter *Cash App User Agreement*]. Cash App is entitled to any interest accrued on those funds. As of the publication of the Article, Circle does not disclose how it treats consumer funds.

97. Bryce Elder, *Circle's stablecoin banked at SVB and guess what happened next*, FIN. TIMES (Mar. 11, 2023), https://www.ft.com/content/7c9b2234-c298-4508-b59a-fce49f6bc40a [https://perma.cc/34X4-62VK].

98. Venmo offers pass-through insurance for certain balances *if* the customer uses certain services, such as direct deposit, check-cashing, and crypto trading. *Venmo User Agreement*, *supra* note 96. Block establishes pass-through insurance for certain balances *if* the customer uses certain products, such as the Cash App card offered with Wells Fargo or children's accounts sponsored by their parents. *Cash App User Agreement*, *supra* note 96. Neither Coinbase nor Circle offer pass-through insurance.

account at a bank on behalf of a principal.[99] However, this form of insurance only protects consumers against the failure of the bank holding the funds for the platform money issuer, not the failure of the platform money issuer (or the wallet company, if they are different entities).[100]Federal banking regulators have taken some steps to clarify the criteria for nonbanks to avail themselves of certain bank privileges.[101] Scholars, industry stakeholders, consumer advocates, and policymakers have also debated the creation of OCC "special-purpose banking charters" that might extend some but not all of the rights and responsibilities of a banking charter.[102]

Given the gaps in banking regulation, for the most part, state and federal regulators treat these digital wallet companies as money services businesses (MSBs), equivalent to Western Union and MoneyGram.[103] Under federal law, nonbank payment app companies must register with the U.S. Department of Treasury Financial Crimes Enforcement Network (FinCEN), an exercise the industry considers perfunctory.[104] Federal banking agencies do not supervise or regulate MSBs. Instead, state regulators impose various rules with various levels of strength. Some state regulators subject MSBs to licensing and safety and soundness requirements, including net worth, bonding, and permissible investments.[105] Some states restrict MSB investments to relatively safe assets, but as evidenced by recent bank failures, even those assets can lose value and cause disruptions. Some states have no restrictions. MSB regulation is substantially weaker than federal banking regulation in all of these cases.[106]

Regulators should also be concerned about how quickly platform money moves in and out of the banking system. Colloquially, regulators refer to volatile balances as "hot money." There have been several hot money crises throughout history, arguably including the March 2023 crisis in which SVB, Signature, First Republic, and Silvergate Bank failed. According to FDIC Chair Martin Gruenberg, SVB customers "sought to

99. CONG. RSCH. SERV., IF12079, DIGITAL WALLETS AND SELECTED POLICY ISSUES (Apr. 18, 2022). *See* 11 Fed. Reg. 177A-431, 177A-449 (Sept. 11, 1946).

100. *See generally* Paul T. Clark, *Just Passing Through: A History and Critical Analysis of FDIC Insurance of Deposits Held by Brokers and Other Custodians*, 32 REV. BANKING & FIN. L. 99 (2012).

101. *See, e.g.*, Proposed Guidelines for Evaluating Account and Services Requests, 86 Fed. Reg. 25865 (May 11, 2021).

102. *See generally, e.g.*, David Zaring, *Modernizing the Bank Charter*, 61 WM. & MARY L. REV. 1397 (2020).

103. Awrey, *supra* note 22, at 46.

104. *See* 31 U.S.C. § 5330.

105. Awrey, *supra* note 22, at 46-56.

106. JP Koning, *Let's Stop Regulating Crypto Exchanges Like Western Union*, COINDESK (Nov. 22, 2022), https://www.coindesk.com/layer2/2022/11/22/lets-stop-regulating-crypto-exchanges-like-western-union [https://perma.cc/G3EN-UY2P].

withdraw nearly all" of the bank's deposits in less than 24 hours."[107] He added that "the ease and speed of moving deposits to other deposit accounts or non-deposit alternatives with the widespread adoption of mobile banking" is a development that has increased the banking industry's "exposure to deposit runs."[108]

Some experts have argued that the FDIC helped set the stage for the problems at SVB, Signature, and First Republic significantly loosening deposit broker rules on behalf of tech companies.[109] Following the S&L Crisis (the archetypical hot money crisis), Congress passed the Financial Institutions Reform, Recovery, and Enforcement Act (FIRREA), empowering the FDIC to restrict the facilitation of deposit gathering for misuse by troubled banks.[110] The FDIC's "Brokered Deposit Rule" imposes restrictions on deposit placement in banks not considered "well-capitalized" by the FDIC.[111] Banks that rely more heavily on brokered deposits must hold more liquid assets in reserve—assets that would otherwise be available for other purposes.[112]

In 2020, the FDIC modified the Brokered Deposit Rule to exempt many fintech companies, including companies in the platform money business.[113] Under the rule, fintech companies do not have to restrict their relationships to banks subject to heightened capital requirements, as investment brokers, for instance, must do.[114] The FDIC no longer considers agents or nominees that place customer funds into "transaction accounts" held "to enable transactions" to be deposit brokers.[115]

As platform money flows through the finance and tech sectors, the looming threats of instability also create a risky interface between bank-

107. Martin J. Gruenberg, Chairman, Fed. Deposit Ins. Corp., Oversight of Financial Regulators: Financial Stability, Supervision, and Consumer Protection in the Wake of Recent Bank Failures (May 18, 2023), https://www.fdic.gov/news/speeches/2023/spmay1723.html [https://perma.cc/DJB2-YNDW].

108. *Id.*

109. *See, e.g.*, *Remarks By Assistant Secretary for Financial Institutions Graham Steele at the Americans for Financial Reform Education Fund*, U.S. DEPT. TREASURY (July 23, 2023), https://home.treasury.gov/news/press-releases/jy1648 [https://perma.cc/53T3-BQA3]. *See also* Martin J. Gruenberg, Director, Fed. Deposit Ins. Corp., Statement on the Final Rule: Brokered Deposits and Interest Rate Restrictions (Dec. 15, 2020), https://www.fdic.gov/news/speeches/2020/spdec1520f.html [https://perma.cc/T2PJ-MBQS].

110. 12 U.S.C. § 1831f.

111. 12 C.F.R. § 337.6.

112. Dan Awrey, *supra* note 54, at 749 (2022).

113. Combined Final Rule on Brokered Deposits and Interest Rate Restrictions, FDIC (Dec. 15, 2020), https://www.fdic.gov/news/financial-institution-letters/2020/fil20113.html [https://perma.cc/MBA4-53HX]. *See* Jelena McWilliams, Chairman, FDIC, Keynote Remarks on "Brokered Deposits in the Fintech Age" at the Brookings Institution, Washington, D.C. (Dec. 11, 2019), https://www.fdic.gov/news/speeches/2019/spdec1119.html [https://perma.cc/MGW4-9AV5].

114. FDIC, *supra* note 113

115. *See* Unsafe and Unsound Banking Practices: Brokered Deposits and Interest Rate Restrictions, 86 Fed. Reg. 6742, 6792 (Jan. 22, 2021) (codified at 12 C.F.R. §§ 303, 337).

ing and commerce (notably, the tech sector). For instance, because regulators do not classify Venmo as a bank, nor do they regulate PayPal, its parent company, an e-commerce giant, as a bank holding company (BHC). PayPal does not have to limit its business activities and relationships to those permitted for banks, including with respect to data collection, use, and retention.[116] However, Venmo's parent company could quickly become a node of contagion. In December 2022, PayPal's customer accounts payable totaled nearly $36 billion alone, equivalent to a mid-tier commercial bank.[117] PayPal's balance sheet features many of the same weaknesses as the failed banks.[118] Although the default rule in corporate bankruptcy is that parent companies are not liable for the debts of their subsidiaries, Venmo contracts make clear that Venmo customers have a direct relationship with PayPal and Venmo customer balances are ultimately liabilities of PayPal.[119] PayPal's failure would bring down Venmo and hang consumers out to dry.

Currently, banking regulators have yet to take substantive steps to handle the risks of platform money. I offer a new approach to regulating the sector, focusing on data governance issues that have co-evolved with the instability and volatility of platform money.

III. Data Brokers

Data brokers provide the core infrastructure of open banking, through which platform money flows.[120] They enable payments between banks and fintech companies by transferring consumer data. Data brokers once relied primarily on "screen-scraping"—copying data, including sensitive personally identifiable information (PII), online when a consumer opened an app.[121] Many data brokers now use developer interfaces—predominantly Application Programming Interfaces (APIs), software that integrates data from third-party apps. By signing up for a platform money account, consumers also grant brokers permission to access their bank accounts to retrieve financial data on behalf of the application.

116. Indeed, PayPal's business model focuses on selling e-commerce payment data for targeted advertisements.

117. PayPal Holdings, Inc., Current Report (Form 8-K) (Apr. 27, 2022).

118. Of the $36 billion, PayPal has invested $11 billion in "cash & cash equivalents." It invests another $17 billion of its customer's billions in *available-for-sale debt securities,* including long-term government bonds, commercial paper, corporate debt securities, and more. Koning, *supra* note 106.

119. *Venmo User Agreement*, *supra* note 96.

120. *See generally, e.g.*, Packin, *supra* note 44 (examining data aggregator business relationships).

121. *See Preserving the Right of Consumers to Access Personal Financial Data: Hearing Before the Task Force on Financial Technology of the Committee on Financial Services*, 116th Cong. (2021) (testimony of Chi Chi Wu, Staff Attorney, Nat'l Consumer Law Ctr.) (arguing screen-scraping practices must be legally prohibited).

Once approved, brokers issue a secured token to other companies, which they can use to access structured machine-readable data from the API without revealing consumer credentials.[122] The banking and fintech industries widely consider tokenization a secure authentication method.[123]

As Dan Awrey and Josh Macey argue, data aggregation is fundamentally a platform business—it "bears all the hallmarks of a 'two-sided market in which strong network effects on each side of the market serve to attract users on the other side."[124] Brokers provide fintech companies with access to the customer data that banks possess, which the companies need to offer services. Conversely, they provide customers with access to the services of fintech companies. Network effects drive two-sided platform markets toward concentration.[125] Once the number of buyers and sellers using a broker reaches a critical mass, the broker creates lock-in effects: consumers must choose between using the platforms or foregoing the most open banking services.[126] Generally, brokers provide consumers services free of charge and leverage the user base to profit from the data they share with other companies.

In her scholarship on information platforms, Julie Cohen provides a relatively specific definition of platforms, distinguishing them from marketplaces, exchanges, networks,[127] or infrastructures.[128] For Cohen, a platform is a "site of encounter where interactions are materially and algorithmically intermediated."[129] Platforms provide networks of "would-be counterparties with access to one another and techniques for rendering users legible to those seeking to market goods and services to them."[130] Platforms exploit digital information and communications networks and supply infrastructures that facilitate particular types of interactions. They also establish the boundaries of networks and privatize and discipline infrastructures.[131] In asserting control through legal and technological protocols, platforms become engines of appropriation and particularized value extraction.

---

122. *See Developer Terms of Use*, PLAID (Jan. 19, 2024), https://plaid.com/legal/terms-of-use [https://perma.cc/J85D-VQ4W]

123. *Security,* PLAID, https://plaid.com/en-eu/security [https://perma.cc/386V-ZE23].

124. Awrey & Macey, *supra* note 2, at 5-6. Plaid argues the CFPB should define companies that manage financial data access under § 1033 as "data access platforms" rather than "data aggregators." *See Plaid SBREFA 1033* Comment Letter, Plaid, 10 (Jan. 25, 2023), https://plaid.com/documents/plaid-CFPB-1033-SBREFA-letter.pdf [https://perma.cc/T9HF-9FJB].

125. Awrey & Macey, *supra* note 2, at 48-50 (network effects).

126. *Id.* at 26 (lock-in effects).

127. A network is a mode of organization in which hubs and nodes structure the flows of transactions and interactions. *See* COHEN, *supra* note 30, at 40.

128. Infrastructures are shared resources that facilitate downstream production of other goods. *Id.*

129. *Id.* at 38.

130. *Id.*

131. *Id.* at 48.

Amy Kapczynski builds on Cohen's account, expanding on the conceptual maneuvers bringing about this platform economy.[132] Kapczynski highlights how platform companies take advantage of various background laws, including laws related to privacy, trade secrecy, intermediary immunities, and the First Amendment.[133] Of particular relevance to open banking and platform money—without changes in the law of contracts that blessed digital "click-wrap" agreements, platform power could not have evolved as it has. [134]

This structural focus allows us to zoom out and picture how the platforms, particularly the data brokers, are reshaping financial services. Data brokers are more than intermediaries or even centralized exchanges. Brokers supply the infrastructure for networks of fintech companies and financial institutions (and government agencies) to share access to data to make consumers more legible. In doing so, they also establish the boundaries and possibilities of platform money and exercise discipline within new forms of finance.

In the world of open banking, one company, Plaid, dominates the data broker market. Zach Perret and William Hockey founded Plaid in 2013, after attempting to develop budgeting and bookkeeping software.[135] In late 2013, Plaid raised a $2.8 million seed round from Spark Capital, Google Ventures, and New Enterprise Associates and began to grow quickly.[136]

Plaid now provides API connectivity to more than 12,000 financial institutions and over 5,500 fintech companies in the U.S. alone, including household names like Sofi, Acorns, Marcus, and Lending Club.[137] Plaid has stated that its network covers over 5,000 federal and state-chartered banks and over 4,000 credit unions—virtually the entire U.S. banking system.[138] Plaid's principal U.S. competitors—MX, Yapily, and Yodlee—are less successful by nearly every business metric.

---

132. Amy Kapczynski, *The Law of Informational Capitalism*, 129 YALE L.J. 1460, 1466 (2020)

133. *Id.* at 1466-67 ("Three moves are critical here: the attempt to absorb trade secrets and data as forms of property protected from 'takings' and from government disclosure; the attempt to insulate the activities of data brokers and software companies by claiming that they are purveyors of speech protected by the First Amendment; and the attempt to insulate markets from domestic control by internationalizing key components of the law of informational capitalism."

134. *Id.* at 1503-04. *See also* COHEN *supra* note 30, at 29 (arguing financial institutions have long exploited contract law in building datafied and intermediate enterprises).

135. Alex Konrad, *Fintech's Happy Plumbers*, FORBES, https://www.forbes.com/plaid-fintech/#581f894267f9 [https://perma.cc/CBY8-6QLU].

136. Anthony Ha, *Plaid Raises $2.8M To Make Banking Data More Developer Friendly*, TECHCRUNCH (Sept. 19, 2013), https://techcrunch.com/2013/09/19/plaid-funding [https://perma.cc/5LCS-PZ54].

137. *About us - our mission*, PLAID, https://plaid.com/company [https://perma.cc/Z5GA-KDFA].

138. Awrey & Macey, *supra* note 2, at 190.

At present, Plaid generates revenue from a variety of sources. Plaid claims it does not sell user data to third parties. But the business model is sharing access to transaction data with wallet providers and banks, or otherwise using transaction data to generate products for secondary markets. Depending on the types of products they use, Plaid charges incumbent financial institutions and fintech companies various fees for access to data. These fees include one-time charges for connecting a new customer account to Plaid's API and ongoing charges for each payment, transaction, or exchange of information processed via Plaid's platform.

Plaid's Transactions API gives both Plaid and app developers access to a user's entire transaction and balance history, including geolocation and category for each purchase made.[139] Plaid's other APIs grant access to rich identity information and data about consumer debt, savings, public benefits receipt, tax payments, property, and investments.

Plaid's wealth of transaction, liability, and identity information is helpful for many lines of business. Plaid also sells customer identification solutions to banks, cash-flow underwriting and credit scoring services to lenders, and financial literacy products directly to consumers. Recent events indicate it is now becoming a more comprehensive financial services company.

In essence, the wallet companies partner with Plaid to engage in arbitrage along the banking perimeter, and Plaid accrues benefits for other business purposes, evading banking regulations that usually govern banking affiliates, including information technology companies. Plaid has its hand on the proverbial "master switch" of a new information network.[140]

A. Disrupting Data Governance

Data brokers like Plaid are far more powerful than yesterday's credit bureaus (although Big Three credit bureaus have now acquired data brokers or established data broker subsidiaries).[141] Whereas credit bureaus may identify users by name, date of birth, social security number, current and previous addresses, phone numbers, and employment.[142] They also collect data from government agencies: municipal offices, courthouses,

139. *What data does Plaid access from my financial institution?*, PLAID, https://support-my.plaid.com/hc/en-us/articles/4410324477847-What-data-does-Plaid-access-from-my-financial-institution [https://perma.cc/GXC5-76MG]; *Transactions*, PLAID, https://plaid.com/docs/transactions [https://perma.cc/SG3E-5MXW].

140. *See generally* TIM WU, THE MASTER SWITCH: THE RISE AND FALL OF INFORMATION EMPIRES (2010) (analyzing the history of monopolism in U.S. information industries).

141. *Credit Reporting Agencies Don't Just Report Credit Scores*, TECH POL'Y @ SANFORD (Nov. 9, 2022), https://techpolicy.sanford.duke.edu/blogroll/credit-reporting-agencies-dont-just-report-credit-scores [https://perma.cc/FHP7-UB3X].

142. *What is a credit report?*, CFPB (Sept. 1, 2020), https://www.consumerfinance.gov/ask-cfpb/what-is-a-credit-report-en-309 [https://perma.cc/PV6L-PA4E].

and property registration systems.[143] Brokers may combine this data with other kinds of data, regularly including, but not limited to, e-mail addresses, gender, age, education, profession, income, political affiliation, marital status, and data about children.[144] They also collect records from carceral institutions, including expunged or sealed documents.[145] Data brokers may also build "shadow profiles" of consumers whose data profiles are missing or incomplete based on the information provided by other consumers.

Financial brokers then sell—or otherwise share access to—data and information with financial technology companies, legacy financial institutions, and non-financial companies alike.[146] The more data that data brokers collect, the more attractive they become as business partners to financial services companies.[147]

Data maximization drives the entire fintech industry, not to mention credit reporting and modern financial services in general. However, the sort of data that brokers collect at the edges of the banking system is particularly rich. Tech companies are especially interested in payment data because it is granular, ubiquitous, and necessary.[148] If social media activity says what we "like," payments data provides a clearer picture of what we do. Payments data provides information about how consumers spend money, which suggests patterns of future spending.

Yet financial data governance law is so antiquated and weak that it does not govern how data brokers like Plaid sort, store, score, and share our data. Thus, the data maximization approach also creates consumer risks, especially for data security and privacy.

---

143. *Id.*

144. STAN ADAMS & JOHN MORRIS, JR., CTR. FOR DEM. & TECH., OPEN BANKING: BUILDING TRUST 77 (2021), https://cdt.org/wp-content/uploads/2021/05/CDT-2021-05-25-Open-Banking-Building-Trust-FINAL.pdf [https://perma.cc/VY9B-3BRN]. Ctr. for Dem. & Tech., Comments Regarding CFPB Inquiry Into Big Tech Payment Platforms 3 (Dec. 20, 2021), https://cdt.org/wp-content/uploads/2021/12/CDT-Comments-to-CFPB-on-Big-Tech-Payment-Systems-Docket-No-CFPB-2021-0017.pdf [https://perma.cc/J4PV-59NU].

145. Michele Gilman, *Poverty Lawgorithms: A Poverty Lawyer's Guide to Fighting Automated Decision-Making Harms on Low-Income Communities*, DATA & SOC'Y 13 (2020).

146. *Why Do Banks Share Your Financial Information and Are They Allowed To?*, U.S. GOV'T ACCOUNTABILITY OFF. (Oct. 13, 2022), https://www.gao.gov/blog/why-do-banks-share-your-financial-information-and-are-they-allowed [https://perma.cc/L2ZV-CAC8]. *See also* Penny Crosman, *Is Finra's Dire Warning About Data Aggregators on Target?*, AM. BANKER (Apr. 9, 2018, 4:54 PM), https://www.americanbanker.com/news/is-finras-dire-warning-about-data-aggregators-on-target [https://perma.cc/729J-42HW] (explaining that data "[a]ggregators are almost always a middleman. When you use an online service or app or even a service from a provider that uses aggregation under the hood, there are very few end customers that realize the aggregator is acting on their behalf as their agent.").

147. BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 51-53 (2016).

148. Carrillo, *supra* note 34, at 1211-12.

On the internet, data insecurity is omnipresent, but data maximization compounds insecurity.[149] Companies maximizing payments data collection can attract malicious actors, given the creation of especially rich datasets.[150] They may allow access for both legitimate and illegitimate third parties. More than 4,000 known data breaches have shaken the economy during the last decade,[151] and most of these incidents have occurred in the financial sector.[152] As nearly every adult in the United States has a credit score (whether they have signed up for a credit card or not), it is almost certain that malicious actors have compromised most consumers' data in some fashion.[153]

Most infamously, in 2017, Equifax—now a data broker as well as a credit bureau—leaked approximately 147 million names and dates of birth, 145.5 million SSNs, 99 million physical addresses, 20.3 million telephone numbers, 17.6 million email addresses, and 209,000 payment card numbers and expiration dates.[154] The CFPB and the FTC signed a settlement requiring Equifax to pay $300 million to compensate consumers, arguing consumers have no control over what Equifax does with data but are subject to the consequences of breach.[155]

In practice, though, laws on the books render little accountability for breaches. All fifty U.S. states require companies to notify customers of a breach and provide minimal remedies,[156] but no overarching federal law governs data security. GLBA requires financial institutions to adopt minimum safeguards to protect customer data.[157] However, courts have interpreted GLBA to impose liability only on the party with the last clear

149. Security experts often argue complexity is the enemy of security. *See, e.g.*, BRUCE SCHNEIER, CLICK HERE TO KILL EVERYBODY 133-38 (2018); Andrea M. Matwyshyn, *Cyber!*, 2017 B.Y.U. L. REV. 1109, 1195 (2017).

150. *See* Majority Staff of H. Comm. on Oversight & Gov't Reform, 115th Cong., Rep. on the Equifax Data Breach 18 (2018) (discussing how the massive amount of consumer data held by credit reporting agencies has made them prime attack targets).

151. *Examining the Use of Alternative Data in Underwriting and Credit Scoring to Expand Access to Credit: Hearing Before the Fin. Tech. Task Force of the H. Comm. on Fin. Serv.*, 116th Cong. 14 (2019) (Statement of Prof. Kristin N. Johnson, Tulane Univ. L. Sch.).

152. *See, e.g.*, Jay P. Kesan & Carol M. Hayes, *Liability for Data Injuries*, 2019 U. ILL. L. REV. 295, 303-04 (2019) (noting that between 2005 and 2014, the finance and insurance industries had the highest number of total incidents at 5,512).

153. *See* Seena Gressin, *The Equifax Data Breach: What to Do*, FTC (Sept. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do [https://perma.cc/9FPC-UJ6T].

154. *See CFPB, FTC and States Announce Settlement with Equifax over 2017 Data Breach,* CFPB (July 22, 2019) https://www.consumerfinance.gov/about-us/newsroom/cfpb-ftc-states-announce-settlement-with-equifax-over-2017-data-breach [https://perma.cc/Q2HV-SWYU].

155. *Id.*

156. *See Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGISLATURES (Jan. 17, 2022), https://www.ncsl.org/technology-and-communication/security-breach-notification-laws [https://perma.cc/P75V-8DQZ].

157. 15 U.S.C. § 6801(b)(3).

chance of notifying consumers of a breach or potential breach.[158] As it is difficult to identify this party and assign liability, companies pay damages to consumers rather than proactively invest in security.[159] There is a larger debate about the vulnerability of payment platforms and whether banks, brokers, or payment app services have a responsibility to pay back consumers who have lost money due to fraud.[160]

Data insecurity can lead to privacy violations.[161] Leading scholars have also concluded privacy laws on the books are insufficiently protective of people's data when private technology companies collect it.[162] There is no overarching substantive federal privacy law. Statutory laws (passed before mass surveillance and predictive analytics) are industry-specific and primarily protect against data misuse rather than collection.

At their core, U.S. privacy laws hinge on a shallow theory of contractual consent.[163] When users sign up for a mobile banking app, digital wallet, or even a standard credit card, they agree to security and privacy policies affirming the company's right to use data according to its terms. These contracts, known as "click-through contracts" operate within a "notice-and-choice" regime. As long as the company notifies us about potential data sharing and we click "I agree" to terms we cannot modulate, courts consider companies to have met the standard of consent.[164] More-

158. Kesan & Hayes, *supra* note 152, at 311.

159. *See* Jay P. Kesan & Carol M. Hayes, *Strengthening Cybersecurity with Cyberinsurance Markets and Better Risk Assessment*, 102 MINN. L. REV. 191, 220-22 (2017); Bruce Schneier, *Liability Changes Everything*, SCHNEIER ON SECURITY (Nov. 2003), https://www.schneier.com/essays/archives/2003/11/liability_changes_ev.html [https://perma.cc/A4JQ-XY42].

160. Kristen E. Larson & John L. Culhane, Jr., *Democratic Senators continue to pressure Zelle and other payment apps to change fraud policies*, CONSUMER FIN. MONITOR (Feb. 20, 2024), https://www.consumerfinancemonitor.com/2024/02/20/democratic-senators-continue-to-pressure-zelle-and-other-payment-apps-to-change-fraud-policies [https://perma.cc/Z557-XM9F].

161. *See* Matwyshyn, *supra* note 149, at 1137-42 (defining security as whether technologies can successfully defend their integrity against third-party attackers).

162. *See, e.g.*, Viljoen, *supra* note 8; Kapczynski, *supra* note 132, at 1505-08 (arguing modern surveillance tools are being deployed against a background of material, embedded inequality); Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773 (2020); Elettra Bietti, *Consent As A Free Pass: Platform Power and the Limits of the Informational Turn*, 40 PACE L. REV. 308 (2020); Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics*, 79 MD. L. REV. 439 (2020); COHEN, *supra* note 30; NANCY KIM, CONSENTABILITY: CONSENT AND ITS LIMITS (2019); Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461 (2019); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016).

163. According to the CFPB, nearly all consumer financial products and services it supervises use clickthrough or "form contracts." *Registry of Supervised Nonbanks that Use Form Contracts to Impose Terms and Conditions That Seek to Waive or Limit Consumer Legal Protections*, CFPB (Jan. 11, 2023) https://www.consumerfinance.gov/rules-policy/rules-under-development/registry-of-supervised-nonbanks-that-use-form-contracts-to-impose-terms-and-conditions-that-seek-to-waive-or-limit-consumer-legal-protections [https://perma.cc/2D45-G8KK].

164. For further discussion of click-through consumer contracts, see, for example, MARGARET RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (2012).

over, many of these contracts contain mandatory arbitration provisions, which courts do not review.

Nominally, the GLBA Privacy Rule requires that banks sharing nonpublic personal information about consumers with nonaffiliated third parties provide (a) an opt-out notice and (b) a reasonable period for the consumer to opt-out.[165] However, consumers cannot opt out of data processing by reporting agencies. They rarely opt out of form contracts and cannot negotiate over the terms in any case. Likewise, the GLBA Safeguards Rule requires all non-bank financial institutions to protect certain customer information,[166] but it is unclear if fintech companies and data brokers partnering with banks are in compliance or must comply at all.[167]

Thankfully, the Bureau will soon subject data brokers to supervision under the Fair Credit Reporting Act (FCRA) of 1970.[168] This rulemaking would allow the CFPB to regulate data brokers and conduct supervisory examinations to assess compliance with federal consumer financial law, including FCRA; obtain information about business practices and compliance systems, and detect and generally assess risks to consumers.

While FCRA supervision is a welcome improvement, FCRA is also notoriously outdated. The FCRA provides a list of consumer rights regarding data collection by consumer reporting agencies (CRAs), including the Big Three credit bureaus (Equifax, Experian, and Transunion), as well as some specialty agencies (like tenant-screening agencies) that the CFPB has flagged as cause for particular concern.[169]

"Furnishers" of consumer data must report accurate information[170] and obtain consumer consent before using information for marketing purposes.[171] Consumers have rights to access their credit report,[172] know

165. *Privacy Rule Handbook*, FDIC (Jan. 25, 2001), https://www.fdic.gov/regulations/examinations/financialprivacy/handbook/index.html [https://perma.cc/C8S7-CGCN].

166. 15 U.S.C. § 6805.

167. The FTC has argued the Safeguards Rule applies to companies that receive information about the customers of financial institutions. *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, FTC (Apr. 2006), https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying [https://perma.cc/E4SE-2FP8].

168. Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information, 88 Fed. Reg. 16951 (Mar. 21, 2023).

169. On January 27, 2022, the CFPB published an "updated list" of "financial surveillance companies" that "identifies dozens of specialty reporting companies that collect and sell access to people's data, including individuals' finances, employment, check writing histories, or rental history records, often without their knowledge." *CFPB Identifies Consumer Reporting Companies the Public Can Hold Accountable*, CFPB (Jan. 27, 2022), https://www.consumerfinance.gov/about-us/newsroom/cfpb-identifies-consumer-reporting-companies-the-public-can-hold-accountable [https://perma.cc/4H8V-GQ4Y].

170. 15 U.S.C. §§ 1681s-2(a)(1) (prohibiting "reporting of information with actual knowledge of errors"), 1681s-2(a)(2) (duty of data furnishers to update and correct furnished information).

171. 15 U.S.C. § 1681s-3.

172. 15 U.S.C. § 1681g.

who else accessed their credit report and who used it adversely,[173] attempt to correct inaccurate information, and have specific categories of information removed from their reports, upon request.[174]

Yet, in practice, consumers' credit files and reports frequently contain errors, such as mistaken identities, discharged debts, and obsolete past accounts.[175] Credit files also often are missing information and vary between CRAs.

Theoretically, FCRA is a "permissible purpose" statute that strongly limits financial data collection and sharing.[176] The FCRA nominally restricts data collection to credit, insurance, and employment purposes.[177] CRAs must limit the duration of reporting certain adverse and sensitive data types,[96,] such as medical data. The FCRA's permissible purpose provisions are critical to the statute's protection of consumer privacy practice. However, a consumer reporting agency may furnish a consumer report for a "legitimate business need," which has been defined so extensively that CRAs have significantly expanded the categories of data they may share.[178]

Moreover, there are serious enforcement issues. FCRA enforcement relies heavily on consumers to monitor their credit reports and enforce firms' duties of data security and accuracy.[112] In practice, however, relatively few consumers access their credit reports, and even fewer challenge the accuracy of information in their reports. [113] And while consumers can elect not to have certain types of data shared with CRAs,[114] consumers often fail to exercise this right.[115] Although FCRA contains a private right of action, courts have reduced FCRA to individual rights to correct inaccurate information and receive notices of negative judgment. Since 2016, the Court has held that future harm to individuals from the storage of in-

173. 15 U.S.C. § 1681.

174. *See, e.g.*, 15 U.S.C. §§ 1681s-2(a)(1)I (removal of defaulted student loan information), 1681(e) (removal of name and address from reports furnished for credit or insurance transactions not initiated by the consumer).

175. *Key Dimensions and Processes in the U.S. Credit Reporting System*, CFPB (2012) https://files.consumerfinance.gov/f/201212_cfpb_credit-reporting-white-paper.pdf [https://perma.cc/8ALW-VZ3B].

176. *See* 15 U.S.C. § 1681 (Congressional findings and statement of purpose for FCRA); CFPB, Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information, 88 Fed. Reg. 16951, 16952 (discussing motivations for the enactment of FCRA). *See also* CHI CHI WU ET AL., FAIR CREDIT REPORTING 19-20 (2022). For state laws operating on similar principles, see California Civil Code (Consumer Credit Reporting Agencies Act) 1785.13.6; WU ET AL., FAIR CREDIT REPORTING [5.4, 10.7.5.2-3]. *See, e.g.*, Permissible Purposes for Furnishing, Using, and Obtaining Consumer Reports, 87 Fed. Reg. 41243, 41244 (July 12, 2022). There are also explicit exceptions for government benefits, law enforcement, and other purposes. *See* 15 U.S.C. § 1681b.

177. *Permissible Purposes for Furnishing, Using, and Obtaining Consumer Reports*, CFPB, https://www.consumerfinance.gov/rules-policy/final-rules/fair-credit-reporting-permissible-purposes-for-furnishing-using-and-obtaining-consumer-reports [https://perma.cc/2ZXS-7ZRD].

178. 15 U.S.C. § 1681b.

accurate consumer data by CRAs is not sufficient to constitute a "concrete injury" to satisfy Article III standing requirements to seek damages.[179]

B. Consumer Financial Harms

Emerging literature on digital privacy and data governance helps us understand the risks. The two traditional approaches to informational privacy. Although often pitted against each other, practically speaking, experts writing according to both the *autonomy view* and the *constitutive view* of privacy reject the status quo of privacy law and arguments from both camps can support a robust data minimization approach to platform money.[180]

First, the *autonomy* view depicts privacy as a right to control the process and sharing of information about oneself as an individual.[181] This view centers on consent, albeit often a more substantive vision than what currently defines privacy law. People cannot consent to data collection or use they cannot anticipate or understand. Often, collectors do not even know the destination or eventual use of data at the point of generation.[182]

Under the autonomy view, data brokers and their partners may violate privacy on several grounds.[183] *Consentless collection* itself is a fundamental informational harm.[184] Consent may also be "*sludgy*"—nominally obtained but substantively corrupted,[185] as with many form contracts per the Bureau's policy position.[186] People may suffer *access harms.* For instance, consumers do not have the right to correct brokers' proprietary algorithmic scores, even if the scoring is discriminatory.[187] Individuals may suffer *"reidentification" harms*, intentionally or because of a data breach or hack. Public disclosure of information may lead to *reputational*

179. *See* TransUnion LLC v. Ramirez*,* 594 U.S. 413 (2021); Spokeo, Inc. v. Robins, 578 U.S. 330 (2016).

180. *See* Amy Kapczynski, *The Cost of Price: Why and How to Get Beyond Intellectual Property Internalism*, 59 UCLA L. REV. 970, 1009 (2012) ("[I]n practice both views suggest that protecting informational privacy requires more than relying on formal individual consent.").

181. *See supra* Part III.

182. *See, e.g.*, Hirsch, *supra* note 162, at 453-61; Richards & Hartzog, *supra* note 162, at 1461-78.

183. I borrow this typology from Viljoen, *supra* note 8, at 595.

184. *See, e.g.*, ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967) (defining privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others").

185. *See, e.g.*, Viljoen, *supra* note 8, at 596.

186. *Registry of Supervised Nonbanks that Use Form Contracts to Impose Terms and Conditions That Seek to Waive or Limit Consumer Legal Protections*, CFPB (Jan. 11, 2023), https://www.consumerfinance.gov/rules-policy/rules-under-development/registry-of-supervised-nonbanks-that-use-form-contracts-to-impose-terms-and-conditions-that-seek-to-waive-or-limit-consumer-legal-protections [https://perma.cc/2D45-G8KK].

187. *Id.*

harm, including stalking, harassment, or shame.[188] Data dumps may engender intimidation or humiliation.[189] These violations may rise to the level of *dignity harms*—spiritual wrongs, assaults upon "inviolate personality," including discriminatory treatment.[190] All of these harms may chill self-expression or economic activity such as participation in open banking.[191] To the extent that certain groups overcome *chilling effects*, they may still suffer *cloaking costs* (for instance, forgoing platform money because of overriding privacy concerns).[192] Courts offer limited remedies for these informational harms, foreclosing the possibility that customers obtain sufficient compensation for injury from collectors.

The *constitutive view* is more capacious than the autonomy view and explicitly analyzes privacy beyond individual impact.[193] For scholars writing according to this view, privacy is not merely a defense against individualized domination. Instead, privacy norms construct, rather than simply reflect, individual preferences, choices, and political values. Mass surveillance alters how we communicate, associate, exchange, and build relationships. Privacy may be necessary for democratic political flourishing.[194] As Julie Cohen argues, protection from attempts to render us "fixed, transparent, and predictable" is vital for informed citizenship, public debate, innovation, and self-governance for democracy itself.[195] The Court itself has recognized privacy as essential to the freedom to associate, organize, and speak meaningfully within social and political groups.[196]

---

188. *See, e.g.*, Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV.373, 374-78 (2009).

189. Remedies for non-pecuniary harms are especially unlikely. *See generally* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793 (2022).

190. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193-220 (1890).

191. *See, e.g.*, Danielle Keats Citron & Jonathon W. Penney, *When Law Frees Us to Speak*, 87 FORDHAM L. REV. 2317, 2318-21 (2019); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1260 (1998) (stating that surveillance can lead to alienation and self-censorship). For a dignitarian theory of surveillance, see SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019). *But see* Kapczynski, *supra* note 132, at 1472-80 (on the limits of Zuboff's dignitarian view).

192. Hirsch, *supra* note 162, at 473-75.

193. *See, e.g.*, Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1 (2021); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426-27 (2000); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1664-66 (1999); Robert C. Post, *The Social Foundations of Property: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 959 (1989).

194. PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 225 (1995).

195. Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1906-11 (2013). *See also* JULIE COHEN, CONFIGURING THE NETWORKED SELF 125 (2012).

196. *See, e.g.*, NAACP v. Alabama ex. rel. Patterson, 357 U.S. 449 (1958) (establishing the compelled disclosure of an NAACP donor database infringed upon freedom of association). *See also* SCOTT SKINNER-THOMPSON, PRIVACY AT THE MARGINS (2020) (identifying a new dimension of "privacy in public," rooted in the First Amendment); Joel Reidenberg, *Privacy in Public*, 69 U. MIA. L. REV. 141 (2014).

Scholars in the constitutive tradition argue that for one person to have privacy (and thus the necessary conditions for self-formation), all of us must have privacy.[197] However, a robust autonomy or dignity view suggests that individual protection is impossible without securing better social conditions for data governance over entire social groups, such as consumers.

I have joined other scholars in shifting from a narrow focus on privacy law towards a more expansive consideration of "data-governance law"—the legal regime that governs how data about people is collected, processed, and used."[198] The goal is not merely to reassert individual control over data collection (although this is a worthy goal). Instead, we should consider the social causes and effects of privacy erosion and how institutions should manage data given those causes and effects.[199]

In previous work, I have detailed broader social and political harms of data maximization in the financial system.[200] Companies may use new datasets and algorithms to hawk new, extractive products.[201] Data brokers may provide commercial datasets to train and maintain harmful automated decision-making systems.[202] These decision systems impact every consumer they interact with, effectively extending the risk of privacy harm and the harm of inaccurate data even to consumers whose data was not collected or used to train the systems.[203] Users have no Fourth Amendment rights in the financial services sector, and law enforcement collects data it might not otherwise be able to collect through the financial system in ways the public does not understand.[204] In particular, private and public institutions deploy surveillance technology that may enhance individual user experiences for the wealthy and comfortable but harms other consumers.

Although financial data brokers like Plaid are not culpable for the broader vacuum of data governance law in the United States, they exploit it, siphoning data along the banking perimeter. In the event of consumer harm, Plaid profits but faces minimal liability. The next section will dis-

197. Viljoen, *supra* note 8, at 600-03.

198. *Id.* at 577-82.

199. *Id*. at 582.

200. *See* Carrillo, *supra* note 34, at 1207.

201. Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information, 88 Fed. Reg. 16951 (Mar. 21, 2023).

202. Consumer financial data can reflect structural racism and bias, leading to the creation of automated decision-making systems that perpetuate racism and bias across private and public applications. *See* Carrillo, *supra* note 34, at 1207.

203. *Id.* at 1231-35; *Press Release*, *NAACP Legal Defense and Educational Fund and Student Borrower Protection Center Announce Fair Lending Testing Agreement with Upstart Network*, NAACP LEGAL DEF. & EDUC. FUND (Dec. 1, 2020), https://www.naacpldf.org/press-release/naacp-legal-defense-and-educational-fund-and-student-borrower-protection-center-announce-fair-lending-testing-agreement-with-upstart-network [https://perma.cc/4AKV-E94V].

204. *See* Carrillo, *supra* note 34, at 1224-26.

cuss why this business model threatens consumers from the perspective of consumer financial protection law.

IV. The Open Banking Rule

Under Director Rohit Chopra, the CFPB has promulgated a rule creating a supervisory regime for payment platforms and is considering rulemaking applying FCRA to data brokers.[205] However, these two rulemakings do not establish any new consumer finance laws.

Most importantly for this Article, in 2020, the Bureau commenced a rulemaking process under section 1033 of the Dodd-Frank Act, which concerns consumers' rights to access financial data and transfer data and funds between banks and fintech companies.[206] In 2023, it proposed a Rule referred to as the "1033," "Financial Data Access," or even simply "Open Banking" rule.

The CFPB centers on a "consumer control" approach—empowering consumers to move funds and data as quickly as possible.[207] The Bureau's proposed rule would require many of the Bureau's covered entities,[208] including banks, to share specific data (transaction and balance information, upcoming bill information, payment initiation information, account terms and conditions, and basic account verification information) and establish obligations for brokers collecting that data.[209] Banks must share data with third parties in an electronic, standardized, credential-free, and machine-readable form.[210]

The proposed Open Banking Rule also establishes a familiar set of consumer rights. Consumers have a right to disclosure of the terms of authorization for data access.[211] Consumers have a right to withdraw con-

205. *See* Proposed Larger Participant Digital Payments Rule, *supra* note 69; CONSUMER FIN. PROT. BUREAU, SMALL BUSINESS ADVISORY REVIEW PANEL FOR CONSUMER REPORTING RULEMAKING, OUTLINE OF PROPOSALS AND ALTERNATIVES UNDER CONSIDERATION (Sept. 15, 2023), https://files.consumerfinance.gov/f/documents/cfpb_consumer-reporting-rule-sbrefa_outline-of-proposals.pdf [https://perma.cc/XZ3G-UCPG] [hereinafter SBREFA OUTLINE].

206. Proposed Open Banking Rule, *supra* note 3.

207. *CFPB Proposes Rule to Jumpstart Competition and Accelerate Shift to Open Banking*, CFPB (Oct. 19, 2023), https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-rule-to-jumpstart-competition-and-accelerate-shift-to-open-banking [https://perma.cc/H7ER-ZE3E].

208. All entities that provide asset accounts subject to Electronic Funds Transfer Act; credit cards subject to the Truth in Lending Act and Regulation Z; and related payment facilitation products and services. *See* Proposed Open Banking Rule, *supra* note 3, at § 1033.111(a)-(c). This definition excludes certain financial accounts, such as mortgage, auto loans, student loans, and EBT accounts, and data aggregators to the extent that they do not provide qualifying financial services. *See id*. at 74803-04.

209. *See id.* § 1033.211.

210. *Id.* § 1033.201(b).

211. Proposed Open Banking Rule, *supra* note 3, at 74796-74801.

sent from third parties for data use.[212] Consumers have a right to request deletion of their data, and companies must delete data if authorization expires after one year.[213]

Beyond these familiar, affirmative consumer rights, the proposed Rule introduces additional data governance principles.[214] The rule bans screen scraping and encourages the use of APIs.[215] The proposed Rule requires banks and third parties to maintain policies and procedures "reasonably designed to ensure the accuracy of covered data made available."[216] The proposed rule extends the GLBA Safeguards Framework to cover third parties explicitly.[217]

Most critically, the CFPB's proposed Open Banking Rule imposes a general data minimization standard: "third parties" (including brokers and wallet companies in the platform money ecosystem) must "limit collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service."[218]

The proposed Rule states the following examples of uses of covered data are "reasonably necessary": uses that are (1) required explicitly under other provisions of law, including to comply with a properly authorized subpoena or summons or to respond to a judicial process or government regulatory authority; (2) reasonably necessary to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; and (3) servicing or processing the product or service the consumer requested.[219]

As an additional defensive measure, the proposed Open Banking Rule establishes bright-line limitations for what does not count as a rea-

212. *See id.* § 1033.421(h).

213. *Id.* § 1033.421(b)(2).

214. Third parties may only *retain* or *use* consumer data beyond that period to the extent "reasonably necessary" to provide the product or service requested by the consumer (defined in terms of the core function and consumer benefit).

215. *See* Proposed Open Banking Rule, *supra* note 3, at § 1033.311(d)(1). *See also id.* at 74800 ("The proposed rule would prevent data providers from relying on screen scraping to comply with the proposal because it is not a viable long-term method of access").

216. *See id.* §§ 1033.351(c) (accuracy obligations for data providers), 1033.421(d) (accuracy obligations for third parties).

217. *See id.* § 1033.311(d)(2).

218. *Id.* § 1033.421(a)(1). The Rule states that, for the purposes of the data limitation standard, a "product or service" will be treated as the "core function that the consumer sought in the market and that accrues to the consumer's benefit." The data minimization standard is similar to standards found in, for example, Competition and Consumer (Consumer Data Right) Rules 2020 div. 1.3 (Austl.) (minimizing consumer data requests to what is "reasonably needed"); Regul. 2016/679, art. 5(1)(c), 2016 O.J. (L. 119) 7 (EU) ("Personal data shall be . . . limited to what is necessary in relation to the purposes for which they are processed.") [hereinafter GDPR]; COLO. REV. STAT. § 6-1-1308(4) (2021) ("A controller shall not process personal data for purposes that are not reasonably necessary to or compatible with the specified purposes for which the personal data are processed, unless the controller first obtains the consumer's consent.").

219. Proposed Open Banking Rule, *supra* note 3, at § 1033.421(c).

sonably necessary business purpose.[220] The collection, use, and retention limits would generally prohibit a third party from using covered data to support targeted advertising, cross-selling other products or services, or selling covered data, even when a customer may have expressly consented to these uses.[221] Companies may offer these products as stand-alone products, however.[222]

The CFPB considered several alternatives to the "reasonably necessary" standard, including "strictly necessary," "adequate," "relevant," or "legitimate."[223] The Bureau claims that the proposed standard would ensure that the consumer is the primary beneficiary of any authorized data access and that data collection, use, and retention align with familiar themes of existing privacy law, especially "informed consent."

A. Industry Response

While the fintech and tech sectors welcome clarity over open banking regulation, many companies are concerned with the "reasonably necessary" standard. Industry stresses that Congress intended the rulemaking to be even more permissive.[224] These challenges telegraph potential legal challenges to the data minimization standard or the Open Banking rule as a whole.

For instance, despite applauding the rule in public, Plaid objects to the data minimization standard and claims "[a] blanket restraint on general product development and improvement – without even allowing for an opt-out or opt-in – is akin to a blanket restraint on innovation and trade."[225]

First and foremost, Plaid argues that the "reasonably necessary" standard "denies consumers meaningful control over their data and many of the benefits third parties can provide."[226] In doing so, Plaid challenges the Bureau's interpretation of informed consent, relying on outdated, heavily critiqued concepts in consumer privacy law. While doing so, it de-

220. *Id.* § 1033.421(a)(2).

221. *Id. See also* Raheel A. Chaudhry & Paul D. Berger, *Ethics in Data Collection and Advertising*, 2 GPH INT'L J. BUS. MGMT. 1, 5-6 (2019) (stating that targeted advertising and data monetization elevate risk the data will be breached or that malicious parties will purchase the data on the secondary market).

222. Accordingly, the proposed rule would not prevent third parties from engaging in an activity described in proposed section 1033.421(a)(2) as a stand-alone product.

223. This standard mirrors other existing open banking standards. *See, e.g.*, *supra* note 218.

224. Christina Tetreault, Comments to the CFPB re: Consumer Access to Financial Records, CFPB (Feb. 12, 2020), https://files.consumerfinance.gov/f/documents/cfpb_tetreault-statement_symposium-consumer-access-financial-records.pdf [https://perma.cc/8N8Z-PR7D].

225. Comment from Plaid, at 71, Plaid (Dec. 30, 2023), https://www.regulations.gov/comment/CFPB-2023-0052-0917 [https://perma.cc/P8BV-JW2A].

226. *Id.* at 3.

nies its role in data maximization and corollary data governance issues, including creating a complex, distributed system with increasingly vulnerable nodes.[227]

While the CFPB considers its rule to be sufficiently flexible to accommodate essential product updates, Plaid argues that under the CFPB Open Banking Rule, consumers cannot reliably count on the express permission for "servicing or processing the product or service the consumer requested"[228] to cover basic anti-fraud and troubleshooting efforts in a complex system.[229] However, the CFPB expressly provides for these types of usage.[230]

Plaid also argues that "fraud" prevention could lead to other types of harm being overlooked, such as money laundering, trafficking, or other harmful activities." However, the Bank Secrecy Act / Anti-Money Laundering regime demands certain types of data collection, use, and retention in its own right. The BSA/AML regime requires an ever-expanding list of "financial institutions,"[231] including payment platforms and financial data brokers, to follow "Know Your Customer" (KYC) requirements by collecting, verifying, and maintaining ID for accountholders.[232] Fintech companies must also file a wide array of reports.[233] Most importantly, they must file "suspicious activity reports" or SARs regarding suspected violations of federal laws against financial flows.[234] However, the proposed Open Banking Rule does not alter these requirements. Although Plaid sells access to a global KYC data platform, Plaid does not need transaction data or need to collect, use, or retain data more data than is strictly necessary to meet KYC requirements in the context of balance transfers.[235]

Second, Plaid seeks refuge in the argument that the data minimization standard will hurt competition and, thus, consumers. Plaid repeats that incumbent data providers (banks) are not subject to any of the rule's

227. *See* Han-Wei Liu, *Shifting Contour of Data Sharing in Financial Market and Regulatory Responses: The UK and Australian Models*, 10 AM. U. BUS. L. REV. 287, 311-12 (2021) ("Although the risks associated with data sharing are not entirely novel, the greater access to data does increase the potential points of cyber-attacks and data breaches.").

228. Proposed Open Banking Rule, *supra* note 3, at § 1033.421(c).

229. *See* Comment from Plaid, *supra* note 225, at 65 ("beyond extremely basic fraudulent activities, preventing fraud in a complex system often depends on access to a wide range of data to enable anomaly detection, learn and identify patterns of fraud, and identify fraudsters operating in multiple areas of a system, among other strategies").

230. *See* Proposed Open Banking Rule *supra* note 3, at § 1033.421(c).

231. *See* 31 U.S.C. § 5312.

232. 31 U.S.C. § 5318(l). *See also* § 31 C.F.R. 1020.220 (banks); 31 C.F.R. § 1022.210 (MSBs).

233. *See* 31 U.S.C. § 5331(a). *See also* 31 C.F.R §§ 1010.410(f); 1010.310-14.

234. 31 U.S.C. § 5318(g)(1). *See also* 31 C.F.R §§ 1020.310 ; 1022.320.

235. *More customers, **minus the fraudsters**,* PLAID, https://plaid.com/products/identity-verification [https://perma.cc/9MAL-UB49].

proposed protections and can liberally market, cross-sell, and otherwise leverage their knowledge of which third-party services their consumers are using. Data providers will construe the Open Banking Rule as giving them discretion to grant or deny access based on pretextual risk management concerns."[236]

Plaid further argues that the prohibition on secondary data use undermines competition by preventing third parties from using covered data "for the development of new products outside the scope of the original authorization."[237] In response, Plaid proposes a data minimization standard explicitly rooted in "the background of existing data privacy laws"[238] (executing one of the informational platform deregulatory "moves" highlighted by Amy Kapczynski).[239]

Plaid argues the CFPB should require third parties to use opt-out terms for data sharing "so long as the secondary use is compatible with the primary purpose in sharing data." As an example of permitted secondary use, Plaid cites marketing or advertising products or services provided by the same company with which the consumer is already a customer like a checking account provider also offering a savings account.

Plaid argues that the CFPB should require third parties to allow consumers to opt into secondary uses beyond those related to the primary purpose. Examples of such uses could include lead generation or marketing by an entity other than the company with which the consumer is already a customer. Secondary compatible uses include, for example, marketing or advertising products or services provided by the same company with which the consumer is already a customer like a checking account provider also offering a savings account.

Opposing the brokers, most legacy financial institutions see the Open Banking rule as too lenient. The American Bankers Association, arguing data brokers "should face even more stringent controls as a separate class because consumers have no meaningful choice—it is purely a business decision by a third party."[240] Furthermore, the ABA argues brokers must accept liability if an eventual third party impermissibly acquires or misuses a consumer's credentials to initiate a fraudulent transaction. It

236. For such concerns, see, for example, Off. of the Comptroller of the Currency, Third-Party Relationships: Interagency Guidance on Risk Management (June 6, 2023), https://www.occ.gov/news-issuances/bulletins/2023/bulletin-2023-17.html [https://perma.cc/ZR8N-X53S].

237. Comment from Plaid, *supra* note 225, at 71.

238. *Id.* at 4.

239. *See supra* Part III.

240. Ryan T. Miller, Re: Docket No. CFPB-2023-0052; Response to Request for Comment on Proposed Rule for Personal Financial Data Rights [RIN 3170-AA78] at 17, 19 (Dec. 29, 2023), https://www.aba.com/-/media/documents/comment-letter/12292023-aba-letter-to-cfpb-re-docket-no-cfpb20230052-nprm-for-personal-financial-data-rights.pdf?rev=d4c43b8966c847efba72da20a3490a87 [https://perma.cc/V8S2-9MLR].

also contends brokers and other third parties should be adequately capitalized and carry sufficient indemnity insurance to satisfy liability obligations.

The Consumer Bankers Association argues the Bureau should prohibit reverse engineering banks' confidential, proprietary information or other trade secrets or making analogous offers to consumers based on observation of the terms of credit accessed through a developer interface.[241] They suggest "copycat underwriting" could raise financial stability concerns.[242]

Akoya, Plaid's bank-owned competitor,[243] has raised concerns that consumers may be distracted and may not be in the best position to assess choices related to their data.[244] Consumers might not take the time to thoroughly review terms and conditions that include broad permission for secondary data uses when their primary interest is in completing the transaction.[245] Akoya proposed an intermediate standard, arguing the CFPB should only permit brokers to use data "as strictly as reasonably necessary" to develop and provide the consumer's requested product or service.

Plaid and allied companies also protest that the CFPB is creating a double standard concerning data governance that undermines competition and innovation. Plaid argues that although data providers like banks collect, use, and retain the consumer same data in the ordinary course of their business, they are subject to GLBA but not 1033 as proposed. Banks can collect, use, and retain data for secondary purposes without a "reasonably necessary" requirement, but Plaid and Venmo cannot do so. Another data broker, Yodlee, also argues that the largest financial institutions in the United States could use consumer data for specific purposes while prohibiting smaller third parties from doing so.[246]

Trade association groups and technology providers are generally anxious to identify industry standards. On June 5, 2024, the CFPB finalized a rule outlining the qualifications to become a recognized industry

241. CBA Comment, at 40-41, Consumer Bankers' Ass'n (Dec. 29, 2023) https://www.consumerbankers.com/sites/default/files/CBA%20Comment%20on%20Docket%20No.%20CFPB%E2%80%932023%E2%80%930052.pdf [https://perma.cc/KA7E-H8SP]

242. *Id.*

243. Originally built by Fidelity, Akoya switched ownership in 2020 to eleven big banks. According to press reports, these banks now seem to be leveraging Akoya to inhibit portability and skim profits off the top of consumers exercising their financial rights. Tom Daniels, *API start-up Akoya becomes joint owned coalition with 11 US banks*, PAYMENT EXPERT (Feb. 20, 2020), https://paymentexpert.com/2020/02/20/api-start-up-akoya-becomes-joint-owned-coalition-with-11-us-banks [https://perma.cc/Z7MP-J25Q].

244. Akoya Comment, at 5-7, Akoya (Dec. 30, 2023), https://www.regulations.gov/comment/CFPB-2023-0052-0879 [https://perma.cc/FBU2-GRTU].

245. *Id.*

246. Yodlee Comment, at 15, Yodlee (Dec. 20, 2023), https://www.regulations.gov/comment/CFPB-2023-0052-0647 [https://perma.cc/RKT6-C74R].

standard-setting body, which can issue standards companies can use to help comply with the CFPB's upcoming Personal Financial Data Rights Rule. The industry argues the CFPB should recognize the Financial Data Exchange ("FDX") industry standard-setting body and create a safe harbor for compliance with qualified industry standards. However, the current FDX standards are significantly broader than the scope of covered data contemplated in the draft rule.[247]

The arguments between the CFPB and industry stakeholders suggest the Opening Banking Rule needs to be stronger, at least concerning the platform money ecosystem. As industry mounts counterarguments, intense litigation and adjudication concerning the unclear "reasonably necessary" standard seems imminent. As Plaid argues, the lack of clarity about routine and worthwhile uses of data creates a high risk of disputes between data providers and third parties as to what data is "reasonably necessary" to be collected, used, and retained, although "[t]he CFPB has preliminarily determined that third parties are in the best position to determine what covered data are reasonably necessary to provide the requested product or service."[248]

Banks will likely seek to narrowly construe the data limitation standard to deny third-party access to consumer financial data. However, brokers are likely to broadly construe the data limitation standard and collect, retain, and use as much consumer financial data as possible. The Bureau mitigates these concerns by providing more detailed guidance on interpreting the data limitation standard and more granular rules limiting presumptively harmful secondary data uses. Yet "targeted advertising," "cross-selling," and "sale" could all have different meanings in different business contexts. Brokers may still use consumer data in ways unintended by consumers.[249]

Zooming out—while the CFPB defends the choice of the "reasonably necessary" standard on the grounds of consumer control, rooted in the individualized notice-and-consent model, data brokers attack the rule on the same grounds. I suggest an alternative model.

To avoid any indication that "reasonably necessary" hinges on consent, the Bureau must decenter the role of consent. Currently, the Bureau stresses individual choice, stating that "consumers are best positioned to understand the scope of that authorization to third-party access to their

247. Akoya Comment, *supra* note 244, at 8-9.

248. Comment from Plaid, *supra* note 225, at 64

249. Some consumer advocates consider this standard sufficient but interpret it as minimizing data collection to "only what is needed for the product or services." This interpretation ignores the "reasonability" element, which will be a locus of contention. *See* Re: Required Rulemaking on Personal Financial Data Rights, Docket No. CFPB-2023-0052/RIN 3170-AA78, NAT'L CONSUMER L. CTR., https://www.nclc.org/wp-content/uploads/2024/01/NCLC-comments-to-Section-1033-NPRM.pdf [https://perma.cc/4XZ3-7KNA].

data and not reluctantly consent to data collection, use, and retention that they do not want."[250]

The Bureau cites EU open banking regulations, defined by the GDPR, and Australian open banking regulations as having comparable minimization standards. In the EU, companies cannot collect data beyond the minimum necessary to provide the service requested by the user, consistent with the data minimization principle set forth by the GDPR.[251] The GDPR restricts data usage at the point of generation, mandates new compliance mechanisms, and provides a set of fundamental user rights.[252] For the most part, however, the GDPR refers to individual dignity harms rather than social harms and still hinges on a gameable conception of consent.[253]

Australian law prohibits a licensed entity from using data beyond what is reasonably required to provide the customer's requested goods or services.[254] Yet it does not limit the types of goods or services involved, and would thus evade regulations such as the CFPB's ban on targeted advertising and cross-selling.[255] In interpreting whether or not the data usage is "reasonably required," it would also turn to a conception of consent and contract law.

Per the CFPB's view of privacy and the 1033 data minimization standard, there is significant room for brokers to argue the collection, usage, and retention of specific data is "reasonably necessary" to achieve a purpose to which an individual consumer consented. For example, under the reasonably necessary standard, brokers might claim they need upcoming billing information, and payment terms and conditions of loans to continue to produce holistic services related to an initial transfer. Plaid encapsulates this reasoning and reveals its thinking by recommending that the CFPB adjust this data minimization standard to include "reasonable and expected" uses of consumer data based on industry standards.[256]

To clarify obligations, the CFPB must depart from its focus on individual consumer control. The Electronic Privacy Information Center

250. *See* Proposed Open Banking Rule, *supra* note 3, at 74833.

251. James Duchesne, John Gevertz, Giulio Coraggio, Cristina Criscuoli & Giorgia Carneri, *US: Open Banking Regulation Arrives in the US*, DLA PIPER (Jan. 17, 2024), https://privacymatters.dlapiper.com/2024/01/us-open-banking-regulation-arrives-in-the-us [https://perma.cc/FJS6-GUAB].

252. *See* GDPR, *supra* note 218.

253. Some scholars have argued the GDPR functionally permits data collection so long as it is deemed valuable for businesses. *See, e.g.*, Waldman, *supra* note 162, at 800-01 (contending risk aversion can incentivize avoidance rather than substantive adherence to the GDPR); Bietti, *supra* note 162, at 337-38 (arguing that as long as we rely on voluntary disclosures and individual choice, we will fail to address the full scope of abusive acts and practices).

254. Scott Farrell, *Embedding Open Banking in Banking Law: Responsibilities, Performance, Risk and Trust*, 17 J. BUS. & TECH. L. 265, 279 (2022).

255. *Id.*

256. Comment from Plaid, *supra* note 225, at 69.

(EPIC)'s letter echoed the need to cull down the categories of required information that could be shared. EPIC argues that while the baseline limitation standard is appropriate for many types of consumer data, the Bureau imposes a more exacting standard for sensitive information, limiting authorized third parties' collection of sensitive consumer data to what is strictly necessary to provide the product or service the consumer has requested (i.e., data without which it is impossible to provide such product or service).[257]

The proposed Open Banking Rule does not refer to more and less "sensitive" types of consumer financial data. Adopting that lens, one might infer that no covered data is sensitive. However, one might also argue that all financial data is sensitive based on what it reveals in the context of larger datasets.[258] The Center for Democratic Technology (CDT) claims the "reasonably necessary" standard is too malleable,[259] but also that financial data is sensitive by any definition. CDT argues CFPB should adopt a more robust "strictly necessary" standard.[260]

Compared to a "reasonably necessary" standard, the "strictly necessary" standard is more prophylactic concerning technological development. The friction associated with embedding more secure and private technology for balance transfer leaves room for brokers to argue more data-intensive legacy technology is "reasonably necessary." With a "strictly necessary" standard, the Bureau would require third parties to upgrade their technology (per industry standard, as it already suggests).[261]

Although Congress should engage in comprehensive banking and privacy reform, I propose the Bureau ratchet up the proposed "reasonably necessary" standard to a "strictly necessary" standard when data brokers transfer balances between bank accounts and platform money wallets. In the next Part, I argue the Bureau should incorporate this standard

257. Comments of the Electronic Privacy Information Center, at 3, Elec. Priv. Info. Ctr. (Jan. 25, 2023), https://epic.org/wp-content/uploads/2023/01/EPIC-Comment-CFPB-Financial-Data-Rights-Rulemaking-Jan2023.pdf [https://perma.cc/9S7W-N5NJ].

258. *See generally* Viljoen, *supra* note 8. *See also* Daniel J. Solove, *Data is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data*, 118 NW. U. L. REV. 1081 (2024) (arguing for a shift from protecting sensitive data to evaluating the extent of harm from the collection, use, or transfer or data).

259. CDT Comments, at 2, Ctr. Democratic Tech. (Jan. 25, 2023), https://cdt.org/wp-content/uploads/2023/01/FINAL-CDT-Comments-on-CFPB-Sec-1033-Dodd-Frank.pdf [https://perma.cc/8QXN-4VWP].

260. This also mirrors language in the American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022), and the Maryland Online Data Privacy Act of 2024, MD. CODE ANN. INS. § 31-207 (West 2024).

261. In theory, Plaid already designs its products to minimize the data accessed to what is reasonably necessary for a defined use case. Comment from Plaid, Comment from Plaid, *supra* note 225, at 64. In situations where over-collection is not avoidable due to technical limitations with the integration with the data provider(s), Plaid's integrations adopt a "filter and purge" approach. This means that excess data is immediately discarded (i.e., not stored), and thus is not passed to the customer or used by Plaid for any purpose. *Id.* at 10.

into the 1033 rulemaking, declaring it a brokers' data mining of simple balance transfers to be an unfair, deceptive, and abusive practice. Alternatively, the Bureau may engage in a different rulemaking process to regulate the behavior of brokers at the banking perimeter.

V. Unfair, Deceptive, and Abusive Practices

Congress established the Bureau to respond to systemic harms beyond prudential banking regulation: primarily predatory lending leading to the 2007-2008 Global Financial Crisis.[262] Lenders originated a disproportionate share of subprime mortgages for Black and Latine households and in predominantly Black and Latine neighborhoods, often in a racially discriminatory manner.[263] Originators sold these loans, which served as the grist for the mortgage-backed securities market that collapsed and took down high finance with it.

Just before the collapse, then law professor and now Senator Elizabeth Warren advanced a proposed single consumer financial protection agency, which would become the CFPB.[264] In Warren's vision, the agency would combine the FTC and banking regulators' authorities to prohibit unfair and deceptive practices.[265] In 2010, Congress passed the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank), which created the CFPB, transferred the authorities, and empowered the Bureau with organic authority to regulate most financial services providers.[266] The Bureau may now prescribe rules identifying and preventing unfair, deceptive, as well as abusive acts or practices.[267] The power is explicit, expansive, and flexible. Other government agencies' interpretations, precedents, and opinions do not bind the Bureau concerning UDAAP.

The Bureau should amend its 1033 proposal to declare:

> **When transferring a balance between the accounts of FDIC-insured depository institutions and stored value accounts, it is an unfair, deceptive,**

262. *See generally* Adam J. Levitin, *The Politics of Financial Regulation and the Regulation of Financial Politics: A Review Essay*, 127 HARV. L. REV. 1991 (2014).

263. *See, e.g.*, Emma C. Jordan, *The Hidden Structures of Inequality: The Federal Reserve and a Cascade Of Failures*, 2 U. PA. J. L. & PUB. AFFAIRS 107, 110-11 (2017); Emma Coleman Jordan & Creola Johnson, *The Magic of Group Identity: How Predatory Lenders Use Minorities to Target Communities of Color*, 17 GEO. J. POVERTY L. & POL'Y 165 (2010).

264. Elizabeth Warren, *Unsafe at Any Rate*, DEMOCRACY (Summer 2007), https://democracyjournal.org/magazine/5/unsafe-at-any-rate [https://perma.cc/3UBT-N2BU]; Oren Bar-Gill & Elizabeth Warren, *Making Credit Safer*, 157 U. PA. L. REV. 1 (2008). For more on the role of politics and organizing behind the CFPB, see Luke Herrine *Unfairness, Reconstructed*, 42 YALE J. ON REGUL (forthcoming 2025).

265. Herrine, *supra* note 264.

266. *See* 12 U.S.C. § 5481(14).

267. 12 U.S.C. § 5531(b).

and abusive practice for a data aggregator to collect, use, or retain more data than is strictly necessary to transfer that balance in compliance with existing laws.[268]

The CFPB already defines "data aggregators" (which I refer to as data brokers) as a distinct class of "third party" within its proposed rulemaking.[269] The Bureau uses the term stored value account to refer primarily to the types of platform money I discuss in this Article, but also includes, for instance, some prepaid debit cards (which lie beyond the scope of this Article).[270]

The CFPB would consider the costs and benefits of my proposal in the context of a broader rulemaking under two different requirements. Under the unfairness rulemaking authority,[271] the Bureau must find that countervailing benefits to consumers or competition do not outweigh injuries to consumers.[272] Per the Bureau's general rulemaking authority, it must consider "the potential benefits and costs to consumers and covered persons, including the potential reduction of access by consumers to consumer financial products or services resulting from such rule."[273] I discuss the unfairness of cost-benefit analysis in the following subsection. At the end of the Part, I comment on the potential impact of my rule on the CFPB's 1033 general rulemaking cost-benefit analysis.

Below, I offer a theory of consumer harm to inform supervision, enforcement, and rulemaking.[274] Practices can be unfair, deceptive, abusive, or any combination of the three.

---

268. Parallel to the 1033 Rule, data collection, use, and retention would be "strictly necessary" if it were (1) required explicitly under other provisions of law, including to comply with a properly authorized subpoena or summons or to respond to a judicial process or government regulatory authority; (2) strictly necessary to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; and (3) strictly necessary for servicing or processing the product or service the consumer requested.

269. The CFPB is proposing to define the term data aggregator to mean an entity that is retained by and provides services to the authorized third party to enable access to covered data. Proposed Open Banking Rule, *supra* note 3, at 74807.

270. In its official regulations, due to the legacy of terms used in the EFTA, the Bureau refers to digital wallet accounts holding funds as stored value accounts. *See, e.g.*, *Analysis of Deposit Insurance Coverage on Funds Stored Through Payment Apps,* CFPB, https://www.consumerfinance.gov/data-research/research-reports/issue-spotlight-analysis-of-deposit-insurance-coverage-on-funds-stored-through-payment-apps/full-report [https://perma.cc/F6B9-VF3Y].

271. Under White House Executive Order 12,866, most executive agencies must "assess all costs and benefits of available regulatory alternatives, including the alternative of not regulating." While the order exempts independent agencies, including the CFPB. *See* Exec. Order No.12,866, 58 Fed. Reg. 51735 (Sept. 30, 1993). The Paperwork Reduction Act exempts "independent regulatory agencies." 12 U.S.C. § 5491(a) (2012).

272. *See* 12 U.S.C. § 5531.

273. 12 U.S.C. § 5512(b)(2). The Bureau must also consider the impact of rulemaking on rural consumers. *Id.*

274. *See also* Phillips & Bruckner, *supra* note 25, at 226 (arguing the CFPB should invoke the abusiveness authority to impose prudential financial requirements upon the likes of Venmo and Cash App); Comment from Raúl Carrillo, Rohan Grey & Luke Herrine to CFPB

A. Unfairness

The Bureau may declare a practice unfair when (1) it causes or is likely to cause substantial injury to consumers, (2) the injury is not reasonably avoidable by consumers, and (3) the injury is not outweighed by countervailing benefits to consumers or competition.[275] The Bureau can also invoke public policy considerations established by statute, regulation, judicial decision, or agency determination but cannot consider them the primary basis for rulemaking.

As discussed at a general level in Parts II and III, the unregulated proliferation of platform money is likely to cause or exacerbate substantial financial and informational injuries to consumers. Consumers cannot reasonably avoid these injuries: they hardly know data brokers exist and cannot meaningfully consent to data collection within the vacuum of data governance law. Moreover, in order to avoid data collection by brokers, consumers would have to forego the use of platform money, as well as many other open banking services. Even if the Bureau stipulated some of the benefits of platform money to consumers, the risks of systemic harm outweigh those benefits.

Substantial injury can involve monetary or reputational harm. In certain circumstances, emotional impacts may amount to or contribute to substantial injury.[276] Critically, actual injury is not required. A significant risk of harm may also suffice. Moreover, a substantial injury to consumers could cause "small harm to a large number of people."[277] Accordingly, the CFPB has asserted that acts and practices with a significant risk of substantial injury to many people satisfy this prong. In analyzing whether an injury is substantial, the Bureau considers the combined likelihood and potential magnitude of harm. The Bureau's headline case against Equifax concerns history's most important consumer data breach and illustrates the principle.

In September 2017, Equifax revealed hackers had exploited the vulnerability to steal over 140 million names, dates of birth, and SSNs, as well as millions of telephone numbers, email addresses, and physical addresses, and hundreds of thousands of credit card numbers and expiration

(Dec. 21, 2021), https://www.regulations.gov/comment/CFPB-2021-0017-0092 [https://perma.cc/5KK7-4M68] (arguing for the CFPB to monitor payment platforms for UDAAP violations).

275. 12 U.S.C. § 5531(c).

276. For instance, see the CFPB's official interpretation of 12 C.F.R. Part 1006. *Prohibition of Unfair, Deceptive, or Abusive Acts or Practices in the Collection of Consumer Debts*, CFPB (July 10, 2013), https://files.consumerfinance.gov/f/201307_cfpb_bulletin_unfair-deceptive-abusive-practices.pdf [https://perma.cc/ZQ3G-4VN4].

277. Letter from Michael Pertschuk et al., Comm'rs, FTC, to Sens. Wendell H. Ford & John C. Danforth, FTC Policy Statement on Unfairness n.12 (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness [https://perma.cc/2CEY-7TCJ]. Federal Trade Commission Act Amendments of 1994, §§ 5, 9, Pub. L. No. 103-312, 108 Stat. 1691, 1695 (1994), codified at 15 U.S.C. § 45(n).

dates. After the notorious incident, the Bureau alleged that in numerous instances, Equifax failed to provide reasonable security for the sensitive personal information of consumers within Equifax's computer networks.[278] The CFPB treated inadequate data security measures as likely to cause substantial injury even without a breach. Indeed, while some claims in the Equifax action focused on the breach that had already occurred, others focused on the *likelihood* that the ensuing security breach response would potentially expose millions of consumers to additional security risks and ID theft.[279]

Although far superior to screen-scraping programs, APIs still suffer from platform vulnerabilities. Even if an individual company prioritizes privacy and security, it is impossible to ensure every other company that it shares data with will follow the same principles.[280] In a "super app," a hacker can cycle through data until they find credentials that work.[281] Malicious actors may hack data brokers to facilitate account takeovers.[282] They can alter or remove large datasets and publish fraudulent data sets. Data collection is accelerating so quickly that it is only a matter of time before consumers are harmed.

The CFPB should similarly address the *likelihood* of small injuries to many people in the platform money context. The data brokers support and perpetuate a fragile and insecure platform money system. If anything, new apps stand to make fraud worse and more frequent.[283] According to Pew Research, about 10% of digital wallet users say they have fallen victim to scams or hacking (a far higher percentage than bank account users).[284] These adverse experiences are more prevalent among certain groups. Still, to worse effect, Black and Hispanic Americans who use payment platforms (22% each) are about twice as likely as their White counterparts (10%) to say they have sent money to someone and later

278. Bureau of Consumer Fin. Prot. v. Equifax Inc., 2019 WL 3287214 (N.D. Ga. 2019).

279. *Consumer Financial Protection Circular 2022-04*, CFPB (Aug. 11, 2022), https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information [https://perma.cc/8PJT-2UKM] [hereinafter *CFPB Circular*].

280. *See, e.g.*, Kristin N. Johnson, *Cyber Risks: Emerging Risk Management Concerns for Financial Institutions*, 50 GA. L. REV. 131, 132-33, 137-39 (2015).

281. Elizabeth Boison & Leo Tsao, *Money Moves: Following the Money Beyond the Banking System*, 67 DOJ J. FED. L. & PRAC. 95, 116 (2019).

282. Kenneth A. Blanco, Director, FinCEN, Identity: Attack Surface and a Key to Countering Illicit Finance, Address at the Federal Identity (FedID) Forum and Exposition (Sept. 24, 2019), https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-federal-identity-fedid [https://perma.cc/W2PC-78H5].

283. When an individual's lifetime of data must be exported "without hindrance," then one moment of identity fraud can turn into a lifetime breach of personal data. Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique,* 72 MD. L. REV. 335, 380 (2013)

284. Anderson, *supra* note 12.

realized it was a scam.[285] Black and Hispanic users are also more likely than White users to say they have had their accounts hacked. There are also differences in household income: some 20% of lower-income consumers surveyed who have ever used these payment apps or sites say they have been the target of scams or hacks, compared with about 10% or fewer users from middle- or upper-income households.[286]

Most critically, new technology increases the likelihood of the composite harm of identity theft or "identity fraud" (the appropriation and use of someone else's identity).[287] Fraudsters may use stolen identity to open a utility account, file a false tax return, or apply for public benefits, housing, or employment, or incur unsustainable credit card debt, leading to lower scores, debt collection lawsuits, wage garnishment, and frozen bank accounts for victims.[288] Victims may lose much-needed income, public benefits, tax refunds, employment, housing, health care, and other necessary services for months or years.[289] If caught committing crimes, fraudsters may even present a false ID with a criminal history to authorities upon arrest, augmenting punishment for people with criminal records.[290] Identity fraud may lead to severe physical and mental health morbidities.[291] Recovery from broader impacts may take years (if recovery is possible at all).[292]

As Sara Greene and Michele Gilman argue, despite conventional wisdom, identity harm is often worse for low-income people precisely because of their low-income status.[293] Thieves may target low-income identities because they can use them for a long time before being detected and stopped.[294] Poor people, especially poor Black people, are typically less able to resolve identity fraud than wealthier people.[295] The laws protecting consumers from identity fraud are thin. The Fair and Accurate Credit

285. *Id.*

286. *Id.*

287. *Identity Theft*, DEP'T OF JUST. (June 9, 2015), https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud [https://perma.cc/962A-M62M]; *Identity Theft: What Can You Do to Protect Yourself?*, NAT'L SCI. FOUND. OIG 1 (2016), https://www.nsf.gov/oig/_pdf/brochures/identitytheft.pdf [https://perma.cc/5CPH-7V5A] (detailing various ways fraudsters use stolen identities).

288. *See generally* Sara S. Greene, *Stealing (Identity) from the Poor*, 106 MINN. L. REV. 59 (2021) (employing rigorous, qualitative empirical methods to identify harms suffered by low-income victims).

289. *Id.* at 80.

290. *Id.* at 79.

291. Davies Burnes et al., *Risk and protective factors of identity theft victimization in the United States*, 17 PREVENTIVE MED. REP. 101058 (2020).

292. *See* Greene, *supra* note 288, at 76-77.

293. *Id.* at 65. *See also, e.g.*, Michele Estrin Gilman, *Me, Myself, and My Digital Double: Extending Sara Greene's* Stealing (Identity) from the Poor *to the Challenges of Identity Verification,* 106 MINN. L. REV. HEADNOTES 301, 307-10 (2022).

294. Greene, *supra* note 288, at 76-77.

295. *Id.* at 68-69.

Transactions Act of 2003 establishes remedial rights for identity theft victims but does little to prevent the crime.[296] The FTC collects reports per its authority under GLBA, but this rarely leads to sufficient repair.[297] Most importantly, many companies require a police report (or even criminal prosecution) before any administrative hearing or civil process.[298] Even if local police are interested in dealing with time-consuming identity fraud cases, members of specific communities often won't report fraud given their distrust of the police.[299] People with limited English proficiency, computer access, or legal representation (groups the CFPB discusses in its 2021 unfair discrimination supervisory manual) may also face difficulty filing a police report. In other words, many consumer groups that the fintech industry targets for "financial inclusion" are least capable of shouldering surveillance harms.

Consumers cannot *reasonably avoid* platform money injuries or the likelihood of those injuries. Analysis of the "reasonably avoidable" element focuses on "whether the consumers had a free and informed choice"[300] and the means to anticipate the impending harm and avoid it."[301]

Longstanding precedent in consumer law holds that injury is also not reasonably avoidable if a company forces consumers to make a specific choice, such as buying unwanted products or services.[302] Venmo, Cash App, and Coinbase customers cannot avoid a third-party relationship with data brokers if they want to use those products.

Moreover, consumers still know little about the brokers.[303] Consumers rarely, if ever, grasp the informational consequences of using fintech

296. 15 U.S.C. § 1681-81x.

297. Greene, *supra* note 288, at 96-98.

298. *Consumer Credit Reporting: Assessing Accuracy and Compliance: Hearing Before the Subcomm. on Oversight & Investigations. of the H. Comm. on Fin. Serv.*, 117th Cong. 7 (2021) (Statement of Chi Chi Wu, Staff Attorney, Nat'l Consumer Law Ctr.).

299. Greene, *supra* note 288, at 99-100, 112.

300. FTC v. Neovi, Inc., 604 F.3d 1150, 1158 (9th Cir. 2010).

301. Consumer Fin. Prot. Bureau v. Navient Corp., No. 3:17-CV-101, 2017 WL 3380530, at *21 (M.D. Pa. 2017). Further, a court will not assume that consumers to whom a business made disclosures "understood the disclosures . . . so that they had 'reason to anticipate the impending harm and the means to avoid it.'" *Id*. (citations omitted).

302. Pa. Funeral Dirs. Ass'n, Inc. v. FTC, 41 F.3d 81, 91 (3d Cir. 1994). FTC v. I.F.C. Credit Corp., 543 F. Supp. 2d 925, 946 (N.D. Ill. 2008) (citing an FTC report to Congress, H.R. Rep. No. 156, pt. 1 (1983)) (emphasis added).

303. *See, e.g.*, FTC Data Brokers Report, at v ("Consumers may not be aware that data brokers are providing companies with products to allow them to advertise to consumers online based on their offline activities"); NCLC, Coalition Letter to CFPB Requesting Broad Consumer Financial Market Correction, Beginning with an Advisory Opinion Regarding Credit Header Data 3 (Feb. 8, 2023), https://www.nclc.org/wp-content/uploads/2023/02/2023-02-08-Coalition-Letter-to-CFPB.pdf [https://perma.cc/96Y2-AXN7] ("Data brokers buy and sell hundreds of millions of names and addresses gathered by essential utilities companies without consumers' knowledge or consent").

apps compared to banking products.[304] Indeed, in a December 2021 survey, The Clearing House—a payments company collectively owned by the largest U.S. commercial banks—found that 80% of consumer respondents were largely unaware that fintech app providers partner with brokers to collect other financial data; 76% did not know brokers can sell that data to other parties; and 78% did not know brokers regularly access personal data even when the app is closed or deleted.[305]

One might counter that consumers could easily spend more time researching or paying closer attention to the terms of their form contracts.[306] Yet the empirical literature says consumers do not read these contracts due to their length and complexity.[307] Scholars have argued such a task would occupy the entire day of the average digital consumer. It is unreasonable to expect consumers to properly construe the terms of multiple contracts involved in a basic balance transfer. The substance of the terms would remain the same. Consumers cannot amend these contracts. Many contain mandatory arbitration provisions. Refusing to agree would shut the consumers out of the services they actually want (such as using a digital wallet to make payments). A choice between two harms does not involve "reasonably avoidable" harm.[308]

Consumers do not necessarily understand the implications of agreeing to boilerplate terms-of-service, even if they are explicit, let alone have the capacity to avoid them.[309] Consumers typically need help knowing whether appropriate security measures are up to code, irrespective of the disclosures provided. Consumers lack the practical means to avoid data security breaches.[310]

304. CREDIT SUISSE, PAYMENTS, PROCESSORS, AND FINTECH, EQUITY RESEARCH REPORT 112 (2021), https://plus.credit-suisse.com/rpc4/ravDocView?docid=V7pyBo2AN-8SW [https://perma.cc/E5XD-CSZ8].

305. THE CLEARING HOUSE, 2021 CONSUMER SURVEY: DATA PRIVACY AND FINANCIAL APP USAGE 3 (Dec. 2021), https://www.theclearinghouse.org/-/media/New/TCH/Documents/Data-Privacy/2021-TCH-ConsumerSurveyReport_Final [https://perma.cc/L3CK-9W65].

306. *See, e.g.*, Ella Corren, *The Consent Burden in Consumer and Digital Markets*, 36 HARV. J.L. & TECH. 551, 568-76 (2023) (arguing the informational ex ante burden in digital markets is unreasonable, and the potential of disclosure to facilitate rational informed consent is very low).

307. For a canonical citation, see, for example, Ian Ayres & Alan Schwartz, *The No-Reading Problem in Consumer Contract Law*, 66 STAN. L. REV. 545, 546-48, 566, 582 (2014).

308. For similar analysis, see, for example, Rory Van Loo, *Helping Buyers Beware: The Need for Supervision of Big Retail,* 163 U. PA. L. REV. 1311, 1371 (2015).

309. *Cf.* Statement of Policy Regarding Prohibition on Abusive Acts or Practices, 88 Fed. Reg. 21883 (Apr. 12, 2023); *Policy Statement on Abusive Acts or Practices*, CFPB (Apr. 3, 2023), https://files.consumerfinance.gov/f/documents/cfpb_policy-statement-of-abusiveness_2023-03.pdf [https://perma.cc/9D6J-DX5H].

310. FTC v. Neovi, Inc., 598 F. Supp. 2d 1104, 1115 (S.D. Cal. 2008) ("[C]onsumers who had their bank accounts accessed without authorization had no chance whatsoever to avoid the injury before it occurred."). *See also* Swire & Lagos, *supra* note 283, at 373-75 (arguing any individual right in the area of data portability should thus be considered together with the individual's right for the data to be protected securely). Pieter T.J. Wolters & Bart P.F. Jacobs, *The Security of Access to Accounts Under the PSD2*, 35 COMP. L. & SEC. REV. 29, 30 (2019) (arguing that

The same reasoning applies to data privacy. Improved disclosure about general practices would also be insufficient, as consumers cannot make an informed choice between products if the relative harms are fundamentally unknowable.[311] Especially within an ever-expanding network of partners and third-party affiliates with such malleable policies, we cannot reasonably expect consumers to track how data brokers buy and sell their data. On an even deeper level, the problem lies in the fact that predictive analytics, by its very nature, infers latent information from surface data. When individuals provide the surface data, they cannot know what latent information they are also revealing. Since individuals cannot understand what their data might reveal in advance, they can no longer "reasonably avoid" any injury that such disclosure might cause. There is no immediate change that data brokers can take to reduce the possibility of harm that does not infringe on their profitability.

Finally, the CFPB must determine if countervailing benefits to consumers or competition outweigh the injuries involved.[312] However, the calculation is still difficult and must capture many factors. For instance, the CFPB should consider costs and benefits to groups of consumers, not just individuals. The Bureau must also grapple with the harms and benefits that affect consumers who are situated differently.

First, it is challenging to compare increased benefits to individual consumers against the social harms the business model may cause if we consider benefits to consumers as a group. (It is similarly difficult to compare individual harms and social benefits). Hypothetically, "countervailing benefits" for some platform money consumers include convenience, ease, speed, and access to new payment and stored-value services. However, the CFPB may also consider unfairness to consumers as a whole or to particular groups of consumers. If the CFPB looks at consumers collectively, the picture changes. For example, unfairness law has always been mainly concerned with harms that affect vulnerable communities, and

customers within an open banking system are vulnerable at more points to their information being abused for "identity theft, blackmail, [or] illegal pricing discrimination").

311. The Pew Center's new survey finds mixed views among users on whether these platforms can safeguard people's information from bad actors. About one-third of payment app or site users (34%) say they are a little or not at all confident that payment apps or sites keep people's personal information safe from hackers or unauthorized users. Black users are more skeptical than other groups: 43% say they are only a little or not at all confident that payment sites and apps keep personal information safe from hackers or unauthorized users, compared with about one-third of White or Hispanic users. Roughly eight-in-ten Americans who have never used these apps say they have a little (20%) or no confidence at all (59%) that these services keep people's information safe. *See* Anderson, *supra* note 12.

312. *See* 12 U.S.C. § 5531.

agencies and courts have never found that countervailing benefits outweigh injuries against protected classes of consumers.[313]

There exists insufficient evidence to offset the harms discussed in the rest of the Article. Consumer protection benefits are frequently difficult to quantify, especially for data governance violations. In financial regulation, it is generally harder to quantify benefits in the form of harms avoided than it is to quantify costs.[314] The Bureau must make numerous rulemaking decisions under conditions of radical uncertainty. Under Richard Cordray, the CFPB conducted voluminous, data-intensive cost-benefit analysis studies. However, with certain exceptions, the Bureau did not monetize major benefits and costs or compare cumulative monetized benefits and costs to each other.[315]

My proposal may chill broader open banking activity, including "alternative lending," in the short term. However, this potential impact is already present in the proposed Open Banking Rule, as the CFPB postpones the analysis of personal financial data rights in the context of mortgages, auto loans, and student loans for a second rulemaking.[316] Moreover, as Lev Menand and Morgan Ricks have argued, defense of the banking perimeter should focus on preventing non-bank corporations from "augmenting the supply of bank money or close substitutes therefor," which is imperative for a stable banking system, even if banks "compete with all manner of other financial institutions in the lending markets."[317] Finally, this is the challenge of the CFPB mandate: to draw the line where risk is too significant, even considering countervailing benefits. The leading consumer benefit of platform money is to effectuate faster payments between people with bank accounts, a goal that policymakers and the industry can achieve in myriad ways.[318]

Countervailing benefits to consumers do not outweigh the risks and costs of data maximization in this context.[319] I am unaware of any in-

313. *See, e.g.*, Am. Fin. Servs. Ass'n v. F.T.C., 767 F.2d 957, 972-75 (D.C. Cir. 1985) (discussing the harms the FTC's Credit Practices Rule was designed to mitigate, which were disproportionately visited on poor consumers).

314. Patricia A. McCoy, *Inside Job: The Assault on the Structure of the Consumer Financial Protection Bureau*, 103 MINN. L. REV. 2543, 2586-89 (2019); Howell E. Jackson & Paul Rothstein, *The Analysis of Benefits in Consumer Protection Regulations*, 9 HARV. BUS. L. REV. 197 (2019) (offering a detailed study of how regulatory agencies actually undertake benefit analysis in promulgating new regulations involving matters of consumer finance and other analogous areas of consumer protection.) *See, e.g.*, John C. Coates IV, *Cost-Benefit Analysis of Financial Regulation: A Reply*, 124 YALE L.J. 305 (2015), (arguing that reliable and precise cost-benefit analysis as applied to financial regulation remains elusive).

315. Jackson & Rothstein, *supra* note 314, at 227. For a brief period, the CFPB attempted to impose a strict CBA requirement on itself, with disastrous consequences. Vijay Raghavan, *Consumer Law's Equity Gap*, 2022 UTAH L. REV. 511, 550-52 (2022).

316. *See* Proposed Open Banking Rule, *supra* note 3, at 74803-04.

317. *See* Menand & Ricks, *supra* note 75, at 602-03.

318. *See infra* Part VI.

319. *See* 12 U.S.C. § 5531.

stance in which a court applying an unfairness standard has found that countervailing benefits to consumers outweighed substantial injury caused or likely to have been caused by a company's poor data security practices. Where companies forgo reasonable, cost-efficient measures to protect consumer data, the CFPB expects the risk of substantial injury to consumers will outweigh any purported countervailing benefits to consumers or competition.[320]

It is difficult to weigh the benefits of potentially increased legibility (such as using payment data to create an "alternative lending profile)." However, this is not the service consumers want when they transfer balances from a bank to a Cash App account or vice versa.

Even if individual consumers may think the benefits of consumer reporting systems outweigh the breach risk, consumers cannot assess the possibility of harm. For instance, they cannot estimate the likelihood of a data breach.[321] Indeed, security officials typically only learn about a vulnerability after a breach. To the individual, the probability of a data breach may seem remote. However, as more consumers accept this bargain, data systems aggregate more data, increasing the risk of a breach for each consumer and the public, including its most vulnerable members.[322]

Turning to the second part of the unfairness CBA analysis, the Bureau's rhetoric cheers for competition. Indeed, the CFPB and Plaid agree that open banking should and will enhance consumer control of information given the right guardrails. Yet the CFPB lacks an overarching competition mandate.[323] Rather, the CFPB's intellectual founders and early leaders stressed the uniqueness and value of its "sole focus on consumer financial protection."[324] Like consumer protection and financial stability, consumer protection and competition are distinct missions.[325]

More importantly, the Bureau's competition rhetoric does not accurately describe the platform money sector. In general, competition in the

320. The Equifax breach produced no countervailing benefits to consumers or competition. The Bureau noted Equifax could have provided random PINs or implemented readily available protections to secure the Incident Website from well-known and reasonably foreseeable vulnerabilities at little or no extra cost, and any savings from Defendant's failure to design and implement these security measures did not benefit consumers or competition. *CFPB Circular*, *supra* note 279.

321. *See* Adam J. Levitin, *Pandora's Digital Box: The Promise and Perils of Digital Wallets*, 166 U. PA. L. REV. 305, 338-39 (2018) (arguing that because most consumers cannot distinguish between products on security bases, and this leads to a "market for lemons").

322. *See* SCHNEIER, *supra* note 147, at 235-38.

323. Rory Van Loo, *Making Innovation More Competitive: The Case of Fintech*, 65 UCLA L. REV. 232, 267 (2018).

324. Steven Antonakes, Deputy Dir., CFPB, Address at the Exchequer Club (Feb. 18, 2015), http://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-of-cfpb-deputy-director-steven-antonakes-at-the-exchequer-club [http://perma.cc/6YWQ-AVH6]. *See also* Bar-Gill & Warren, *supra* note 264, at 98-100 (pointing out the drawbacks of subsuming consumer protection under safety and soundness).

325. Van Loo, *supra* note 323, at 273.

financial technology (fintech) sector has evolved far beyond a brawl between start-ups. Many scholars and policymakers refer to an arms race between legacy financial institutions and technology companies. However, these companies also coordinate—the average U.S. bank account now shares data with at least fifteen other finance apps and services, unbeknownst to consumers.[326] According to one 2022 study, nearly two-thirds of banks and credit unions entered at least one fintech partnership over the previous three years.[327] In some contexts, the same companies competing in one industry sphere will collaborate in another sphere.[328]

If the CFPB aims to promote fair competition that benefits consumers, it needs to better define the domain of competition. Although the CFPB does not explicitly identify the markets in which it wants to promote fair competition, its Open Banking Rule focuses on the competition between banks and their direct competitors in the infrastructure for payments, lending, and deposits or their limitations.

The CFPB pays less attention to competition within the data brokerage industry. Consumers want to use the most easily available platform, and all businesses involved want access to platforms with the most consumer data.[329] Companies must spend significant sums to develop their APIs. There are few incentives to entertain a competitor to Plaid. Wallet companies and banks have viewed Plaid's single, standardized API as an attractive alternative to proprietary API development or bilateral agreements with different companies. As Plaid itself has explained: "[t]he real shift here is this is standardized, almost open-finance-in-a-box."[330]

This power was on full display when the DOJ sued Visa Inc. when it attempted to acquire Plaid. The DOJ concluded that Plaid's extensive connections with banks and consumers gave Plaid a competitive advantage that other companies could not replicate and that the acquisition was anti-competitive. The DOJ complaint prompted Visa to abandon the proposed acquisition.

Banks still fight the demands for a unidirectional flow of data, arguing that such a one-sided initiative is problematic and serves neither competition nor consumers.[331] However, in May 2021, Plaid began establish-

326. CREDIT SUISSE, *supra* note 304, at 112.

327. RON SHEVLIN, SYNCTERA, THE STATE OF THE UNION IN BANK-FINTECH PARTNERSHIPS 1 (2022), https://19538404.fs1.hubspotusercontent-na1.net/hubfs/19538404/220110%20SYNCTERA%20Bank-Fintech%20Partnerships.pdf [https://perma.cc/52AP-JRV8].

328. *See, e.g.*, Packin, *supra* note 44.

329. Awrey & Macey, *supra* note 2, at 41.

330. Awrey, *supra* note 22, at 188.

331. This consumer-facing bi-directional flow of data is one of the key premises in the Australian CDR, which creates a singular consumer right to access data on their own consumption of goods and services. Packin, *supra* note 44, at 1335-36.

ing bidirectional APIs, which may suggest an alternative path for the industry.[332]

My proposal could impact the structure of the data broker market in at least three different ways. First, Plaid could contract its business model but remain the dominant player, subject to enhanced CFPB regulation and the new data minimization standard. Second, Plaid could remain one competitor in a marketplace that includes many other data brokers and traditional financial institutions creating their APIs, perhaps emphasizing bilateral connections. Third, Akoya or another competitor less invested in data maximization could become the dominant player under new standards. The CFPB should prefer any of these outcomes to the status quo, defined by banking law arbitrage and data maximization.

B. Deceptiveness

Deceptiveness is one of the most commonly pleaded claims in consumer protection cases.[333] A representation, omission, or practice is "deceptive" if: (1) the representation, omission, or practice misleads or is likely to mislead the consumer; (2) the consumer's interpretation of the representation, omission, or practice is reasonable under the circumstances, and (3) the misleading representation, omission, or practice must be material.[334]

Misleading representations "may be in the form of express or implied claims or promises and may be written or oral."[335] An omission may be deceptive if disclosure would be necessary to prevent a consumer from being misled.[336] Further, representations and omissions are evaluated in the context of the entire advertisement, transaction, or course of dealing—rather than in isolation—to determine whether they are misleading.[337]

The materiality of a representation, omission, or practice is assessed based on whether "it is *likely* to affect a consumer's decision to purchase or use a product or service."[338] An intent to deceive is not required. Rather, if the Bureau could show that the institution "intended that the con-

---

332. Alex Hamilton, *US Bank and Plaid sign third party API integration deal*, FINTECH FUTURES (May 17, 2021), https://www.fintechfutures.com/2021/05/us-bank-and-plaid-sign-api-integration-deal [https://perma.cc/G5SF-LCE3].

333. *CFPB Circular*, *supra* note 279.

334. *See* FDIC CONSUMER COMPLIANCE EXAMINATION MANUAL — JUNE 2022, at VII–1.3, FDIC (June 2022), https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/7/vii-1-1.pdf [https://perma.cc/FLP6-EX5Z] [hereinafter FDIC MANUAL].

335. *Id.* at VII–1.4.

336. *Id.*

337. *Id.*

338. *Id.* (emphasis added).

sumer draw certain *conclusions* based upon the claim," it would presume materiality.[339]

To determine whether an act or practice is misleading, the Bureau adopts the "reasonable consumer" perspective, based on how a reasonable member of the target audience for that product would interpret the marketing material.[41] For example, disclosures buried in the fine print of a consumer contract are "generally insufficient to cure a misleading headline or prominent written representation."

Similarly, brokers will likely mislead consumers regarding how companies use their data. This analysis is implicit in the unfairness analysis for reasonable avoidability. Consumers cannot avoid dangerous data practices they cannot understand or change if they want to.

In its first-ever data security case, the Bureau found that Dwolla, a money transfer platform like Venmo, had engaged in deceptive practices when Dwolla told its customers that its data security protocol "surpass[ed] industry security standards." In reality, Dwolla "failed to employ reasonable and appropriate measures to protect data obtained from consumers against unauthorized access."[340]

Most consumers typically have yet to learn data brokers are even collecting their data. In any case, if a company shares data with third parties and cannot provide any specificity as to the life of the data, they are necessarily making misleading representations. Plaid does this implicitly when it says things like "we don't sell your data" when they do sell *access to user data.*[341]

Proving deception also requires evaluating the purpose of data collection from the perspective of what the average consumer would expect given the context. When a customer grants access to Plaid to transfer cre-

339. *Id.* (emphasis added)

340. *Dwolla, Inc.*, CONSUMER FIN. PROT. BUREAU (Mar. 2, 2016), https://www.consumerfinance.gov/enforcement/actions/dwolla [https://perma.cc/MZ4F-QNNR].

341. *See The safer way to share your financial information*, PLAID, https://plaid.com/safety [https://perma.cc/693Q-NBF8] ("We don't share your personal financial information without your permission, and we don't sell or rent it to outside companies."). Technology companies and regulators have long fought over the definition of "selling" data. Ari Ezra Waldman characterizes this common defense as a "misdirection from all the other ways that may be more subtle but still are deep and profound invasions of privacy." Alfred Ng, *What Does It Actually Mean When a Company Says, "We Do Not Sell Your Data"?*, THE MARKUP (Sept. 2, 2021, 8:00 AM), https://themarkup.org/ask-the-markup/2021/09/02/what-does-it-actually-mean-when-a-company-says-we-do-not-sell-your-data [https://perma.cc/4B35-NZLZ]. Some jurisdictions have responded to this semantic misdirection by changing laws. For instance, privacy advocates pushed the California state legislature to amend the California Consumer Privacy Act law to expand the definition of "selling data" to include any practice by which apps or platforms track user behavior and then share that data for commercial purposes (like targeted advertising on other apps and services). *See, e.g.*, Children's Online Privacy Protection Rule - Notice of Proposed Rulemaking 16 C.F.R. 312 Project No. P195404, Comments of Common Sense Media, COMMON SENSE MEDIA (March 11, 2024), https://www.regulations.gov/comment/FTC-2024-0003-0244 [https://perma.cc/4EZU-QAE6]. Plaid (a California-based company) engages in such services as a fundamental part of its business model.

dentials and money between a bank account and an app, there is no reason for them to imagine companies will use their data for any other purpose than effectuating transfers. The FTC has found it to be a deceptive trade practice for a business to process personal data that it has not disclosed, even if the company has been forthright about other processing it performs on the same data.[342] Disclosures buried in the fine print of a consumer contract are generally insufficient to cure a misleading headline or prominent written representation.[343]

These representations and omissions made in the business of data-brokered deposits are *likely* to affect a consumer's decision to purchase or use mobile apps and thus pass the "materiality" test. Plaid is an adhesive attachment to digital wallets. Consumers must agree to its usage. They might not sign up for the product if they knew how Plaid used their data. An intent to deceive is not a required element.[344] Instead, here we can show that data brokers merely intend for the consumer to draw certain *conclusions* based upon claims the companies make about not selling data.[345]

Plaid has now been accused of taking too much financial data from users and using that information to access and sell their transaction history.[346] A class-action suit alleged that Plaid collected users' bank account login information through web pages that mimicked "the look and feel of the user's own bank account login screen."[347]

According to the lawsuit, the plaintiffs alleged that Plaid has "exploited its position as a middleman" to obtain app users' banking login credentials and use that information to access and sell their transaction histories. These actions occurred without users knowing Plaid's role is a variant of "deceptive tactics." The plaintiffs recounted that they signed up for fintech apps, including Venmo and Cash App, linked their bank accounts, and were unaware of Plaid's role or that the company would collect banking information. However, the judge found the plaintiffs suf-

342. For example, the Commission recently determined that Twitter deceived consumers by using email addresses and phone numbers collected for one purpose (account security) for an undisclosed purpose (targeted advertising). *In re* Twitter, Inc., FTC File No. 202-30623 (2022).

343. CFPB, UNFAIR, DECEPTIVE, OR ABUSIVE ACTS OR PRACTICES 5 (Oct. 1, 2012), https://files.consumerfinance.gov/f/documents/cfpb_unfair-deceptive-abusive-acts-practices-udaaps_procedures_2023-09.pdf [https://perma.cc/V676-UBBM].

344. FDIC MANUAL, *supra* note 334, at VII–1.4.

345. *Id.*

346. Emma Roth, *Plaid, the service used by Venmo, Acorns, Robinhood, and more, may owe you some money*, THE VERGE (Jan. 23, 2022), https://www.theverge.com/2022/1/23/22898009/plaid-financial-venmo-acorns-robinhood-class-action-lawsuit [https://perma.cc/95KS-DFHS].

347. Natalie Hason, *Judge approves settlement ordering Plaid to pay $58 million for selling consumer data*, COURTHOUSE NEWS SERV. (July 20, 2022) https://www.courthousenews.com/judge-approves-settlement-ordering-plaid-to-pay-58-million-for-selling-consumer-data [https://perma.cc/DHY8-CTDK].

ficiently alleged invasion of privacy, violation of California's anti-phishing law, and other claims. In July 2022, the company settled the suit for $58 million without admitting wrongdoing and claimed it was adequately transparent with the user.[348] The court required Plaid to pay affected consumers about $13.50 each.

C. Abusiveness

The CFPA defines an "abusive" act or practice as one that (1) materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service or (2) takes unreasonable advantage of (A) a lack of understanding on the part of the consumer of the material risks, costs, or conditions of the product or service; (B) the inability of the consumer to protect its interests in selecting or using a consumer financial product or service; or (C) the reasonable reliance by the consumer on a covered person to act in the interests of the consumer.[349]

Most importantly, as the Bureau outlines in its policy statement on abusiveness, there is no required showing of substantial injury to establish liability, or cost-benefit analysis involved, the establishment of intent, as the conduct is itself the violation.[350] Consumers need not act reasonably.[351] In more recent policy guidance, the CFPB has described its abusiveness standard as applying when "financial products and services [are] 'set up to fail'" or when providers "benefit from, or [are] indifferent to, negative consumer outcomes."[352] Furthermore, the CFPB has argued the question "is whether some consumers in question have a lack of understanding, not all consumers or even most consumers."[353] Unlike an unfairness claim, an abusiveness claim imposes no cost-benefit analysis.

Abusiveness is about power: Congress focused on prohibiting abusive business models and other acts or practices that benefit a company but harm consumers. Congress created the abusiveness standard by ex-

348. *Id.*

349. The CFPB borrows its definition of abusiveness from the Home Ownership and Equity Protection Act (HOEPA) of 1994, implemented by the Fed Board. Luke Herrine, *The Folklore of Unfairness*, 96 N.Y.U. L. REV. 431, 434 (2021).

350. *Policy Statement on Abusive Acts or Practices*, CFPB (Apr. 3, 2023), https://www.consumerfinance.gov/compliance/supervisory-guidance/policy-statement-on-abusiveness [https://perma.cc/CQF3-J4V9] [hereinafter *Abusiveness Policy Statement*].

351. *See, e.g.*, CFPB v. Access Funding, LLC, 270 F. Supp. 3d 831, 850 (D. Md. 2017).

352. *Abusiveness Policy Statement*, *supra* note 350; Jean Braucher, *Form and Substance in Consumer Financial Protection*, 7 BROOK. J. CORP. FIN & COM. L. 107, 110 (2012) ("The CFPB appears focused on eliminating financial products that are based on tricks and traps, that is, on working to do away with substantively bad, unsafe deals.").

353. *Abusiveness Policy Statement*, *supra* note 350 ("Since there can be differences among consumers in the risks, costs, and conditions they face and in their understanding of them, there may be a violation with respect to some consumers even if other consumers do not lack understanding.").

plaining that if the Bureau had enforced the standard, it would have been able to challenge how mortgage originators and servicers took systematic advantage of borrowers in the subprime mortgage market of the early 2000s, leading to the GFC.[354]

Some scholars and policymakers have suggested that abusiveness harkens back to a more robust definition of unfairness.[355] Other scholars argue that abusiveness is something like an enhanced unconscionability standard.[356] Director Chopra has argued the creation of the abusive practices authority was "in some ways a return to the original framework of consumer protection ingrained in the American tradition."[357] In its first decade, the Bureau has used abusive practices authority to prohibit regulated entities from using the internet or tribal territory to avoid state usury laws,[358] from steering consumers to more expensive financial services,[359] from taking advantage of consumers' limited (or total lack of) alternatives;[360] from knowingly providing services that will not benefit consumers;[361] from designing employee compensation in a way that encourages them to steer consumers to inferior options;[362] and from obscur-

354. Herrine, *supra* note 349, at 527-28.

355. *Id.*

356. *See, e.g.*, Carey Alexander, *Abusive: Dodd-Frank Section 1031 and the Continuing Struggle to Protect Consumers*, 85 ST. JOHN'S L. REV. 1105, 1115-16 (2011) (arguing UDAP statutes and other consumer protection measures are meant to codify the soul of unconscionability doctrine).

357. *Id.*

358. *CashCall* is the leading case. CFPB v. CashCall, Inc., 2016 WL 4820635 (C.D. Cal. Aug. 31, 2016); *see* CFPB v. CashCall, Inc., 2023 WL 2009938 (Feb. 10, 2023) (discussing the procedural history since—in which the CFPB survived all challenges—and granting requested remedy).

359. The leading case is *ITT Educational Services*. CFPB v. ITT Educ. Servs., Inc., 219 F. Supp. 3d 878, 918-21 (S.D. Ind. 2015). According to *ITT Educational Services*, the meaning of "unreasonable advantage" is "broad" and means something akin to unfairly profiting from or to unfairly make use of another for one's benefit. *See also* Complaint, CFPB v. Populus Fin. Grp., Inc., No. 3:22-cv-01494 (N.D. Tex. July 12, 2022); *but see* Alan S. Kaplinsky & Michael Gordon, *Populus Financial Group and CFPB Agree to Stay of CFPB Lawsuit Pending Issuance of Fifth Circuit's Mandate in Decision Holding CFPB's Funding Mechanism is Unconstitutional*, CONSUMER FIN. MONITOR (Nov. 1, 2022), https://www.consumerfinancemonitor.com/2022/11/01/populus-financial-group-and-cfpb-agree-to-stay-of-cfpb-lawsuit-pending-issuance-of-fifth-circuits-mandate-in-decision-holding-cfpbs-funding-mechanism-is-unconstitutional [https://perma.cc/2TXP-SNNW]; *CFPB and Navajo Nation Take Action to Stop an Illegal Tax-Refund Scheme*, CFPB (Apr. 14, 2015), https://www.consumerfinance.gov/about-us/newsroom/cfpb-and-navajo-nation-take-action-to-stop-an-illegal-tax-refund-scheme [https://perma.cc/48NP-66XU].

360. CFPB v. ITT Educ. Servs., Inc., 219 F. Supp.3d 878, 918-21 (S.D. Ind. 2015); Consent Order, *In re* JPay, File No. 2021-CFPB-0006 (Oct. 19, 2021); Complaint, CFPB v. MoneyLion Technologies. Inc., 22-cv-8308 (S.D.N.Y. Sept. 29, 2022); Complaint, CFPB v. Nexus Servs., Inc., No. 5:21-cv-00016 (W.D. Va. Feb. 22, 2021); Complaint, CFPB v. All Am. Check Cashing, 3:16-cv-356-WHB-JCG (S.D. Miss. May 11, 2016); Final Settlement Order, CFPB v. All Am. Check Cashing, 3:16-cv-00356-DPJ-BWR (S.D. Miss. Nov. 10, 2022).

361. Stipulated Final Judgment and Order, CFPB v. Am. Debt Settlement Solutions, Inc., 9:13-cv-80458-DMM (S.D. Fla. June 7, 2013).

362. Complaint, CFPB v. Credit Acceptance Corp., 23-cv-0038 (S.D.N.Y. Jan. 4, 2023); Complaint, CFPB v. Aequitas Cap. Mgmt., Inc., No. 17-1278 (D. Or. Aug. 17, 2017); Stipulated Final Judgment and Order, 17-cv-1278-PK (D. Or. Sept. 1, 2017); Amended Complaint, CFPB v.

ing the cost of financial services through non-obvious pricing structures,[363] among other practices. The Bureau has often paired claims of abusive practice with claims of unfair practices.[364] For years, the Bureau and industry critics have litigated over the Bureau's enforcement-centered approach. However, in April 2023, the Bureau issued a policy statement on abusive acts or practices.[365]

In the business of platform money, regardless of whether they materially interfere with consumer understanding, brokers take unreasonable advantage of (1) a lack of consumer understanding regarding the risks of open banking, (2) the inability of consumers to select a broker, much less protect their interests against that broker, and (3) the reasonable reliance of the consumer that brokers act in their interest.

The Bureau could potentially demonstrate "material interference" and thus abusiveness when a covered entity "impedes consumers' ability to understand terms or conditions, has the natural consequence of impeding consumers' ability to understand, or impedes understanding."[366] However, given the focus on disclosure, the CFPB is better off relying on the other elements.[367] Abusiveness may entail taking unreasonable advantage of three particular circumstances, even if the entity did not create those circumstances. Intentionality is not required.

When there are "gaps in understanding" regarding the material risks, costs, or conditions of the entity's product or service, entities may not take unreasonable advantage of that gap, regardless of how the gap arose.[368] The CFPB does not need to argue that brokers caused the lack of understanding in question.[369]

There is no need to demonstrate that the consumer's lack of understanding was reasonable to demonstrate abusive conduct.[370] Similarly, the

Fifth Third Bank, NA, No. 1:21-cv-262 (S.D. Oh. June 16, 2021). *See also* Consent Order, *In re* Cash Express, LLC, File No. 2018-BCFP-0007 (Oct. 24, 2018) (instructing employees to prevaricate about set-off and disciplining those who failed to do so).

363. Consent Order, *In re* Regions Bank, File No. 2015-CFPB-0009 (Apr. 28, 2015); Consent Order, *In re* Regions Bank, File No. 2022-CFPB-0008 (Sep. 28, 2022); Consent Order, *In re* TD Bank, NA, 2020-BCFP-0007 (Aug. 20, 2020); Consent Order, *In re* Fort Knox Nat'l Co., 2015-CFPB-0008 (Apr. 20, 2015); Complaint, CFPB v. MoneyLion Technologies Inc., 22-cv-8308 (S.D.N.Y., Sept. 29, 2022); CFPB v. ITT Educ. Servs., Inc., 219 F. Supp.3d 878, 918-21 (S.D. Ind. 2015).

364. *E.g.* Complaint, CFPB v. MoneyLion Technologies Inc., 22-cv-8308 (S.D.N.Y. Sept. 29, 2022); Consent Order, *In re* Regions Bank, File No. 2022-CFPB-0008 (Sept. 28, 2022); Complaint, CFPB v. Populus Fin. Grp., Inc., No. 3:22-cv-01494 (N.D. Tex. July 12, 2022).

365. *Abusiveness Policy Statement*, *supra* note 350 (supervisory guidance).

366. *See id.* at n.18.

367. *Id.*

368. *See* 12 U.S.C. § 5531(d).

369. *See Abusiveness Policy Statement*, *supra* note 350 ("While acts or omissions by an entity can be relevant in determining whether people lack understanding, the prohibition . . . does not require that the entity caused the person's lack of understanding through untruthful statements or other actions or omissions.").

370. *Id.*

prohibition does not require proof that some threshold number of people lacked the understanding to establish that an act or practice was abusive.

The Bureau can demonstrate a public lack of understanding of data broker practices based on surveys, complaints, and consumer testimony as discussed throughout this Article and the surrounding literature.[371] The CFPB can also indicate a lack of understanding by considering a course of conduct and likely consequences.

A consumer's "inability to protect" their interests includes situations when it is impractical to protect their interests in selecting or using a consumer financial product or service. The CFPB is mainly concerned with unequal bargaining power and leverage by companies. Such circumstances may occur at the time of, or before, the person selecting the product or service, during their use of the product or service, or both. Consumer "interests" include monetary and non-monetary interests, including but not limited to property, privacy, or reputational interests.

People are often unable to protect their interests when they do not elect to enter into a relationship with an entity and cannot select to enter into a relationship with a competitor. Conduct can be abusive when there is no contractual relationship between the person and the entity, which takes unreasonable advantage of the person's lack of understanding.[372] This lack of transparency allows for cascading harms through downstream misuse of consumer data.[373]

Venmo, Cash App, and Coinbase require their customers to use Plaid. The Bureau has already made clear it is concerned with unequal bargaining power when business partnerships involve unknown. Credit reporting companies, debt collectors, and third-party loan servicers and consumers cannot exercise meaningful choice in interacting with those entities.[374] Consumers often cannot defend their interests when selecting or using a consumer financial product or service where companies have outsized market power, like Plaid.

Finally, entities must refrain from taking advantage of *consumer reliance*. This basis for finding abusiveness recognizes that sometimes people are in a position in which they have a reasonable expectation that an entity will act in their interest to make decisions for them or to advise them on how to make a decision. Where people reasonably expect that a covered entity will make decisions or provide advice in the person's interest, there is potential for betrayal or exploitation of the person's trust.

---

371. *Id.*

372. *Id.*

373. *See, e.g.*, *Fighting Back Data Brokers*, JUST FUTURES LAW, https://www.justfutureslaw.org/fighting-data-brokers [https://perma.cc/PFT2-X67F]; Just Futures Law, Reply Comments in the Matter of Data Breach Reporting Requirements, WC Docket No. 22-21, at 10 (Mar. 24, 2023), https://www.fcc.gov/ecfs/document/10325231325541/1 [https://perma.cc/6DRP-3F53]

374. *See Abusiveness Policy Statement*, *supra* note 350.

Reasonable reliance may exist where an entity communicates to a person or the public that it will act in its customers' best interest or otherwise holds itself out as working in the person's best interest. The entity in these situations creates an expectation of trust and the conditions for people to rely on the entity to act in their best interest.

For instance, in the platform money sector, wallet companies that target or exclude specific consumer groups, including but not limited to protected classes, purposefully foster conditions of reasonable reliance. Given the overwhelming promises of financial inclusion in the space, public policy requires sufficient attention to how the business of platform money impacts consumers based on race, gender, sexuality, class, national identity, immigration status, and other identity factors.[375] Legal scholars and sociologists have suggested that patterns of exclusion leading to unequal inclusion–call it "exploitative inclusion" or "predatory inclusion"—is a characteristic feature of a change in the structure of social provisioning institutions in the United States in the latter half of the Twentieth Century.[376]

Cash App makes racially targeted ads about financial inclusion as part of its business model. Consumer advocates and competitors have accused the company of misconduct it has had a difficult time defending.[377] On March 23, 2023, investment research firm Hindenburg Research disclosed a short position in Block, leading to a 15% drop in the company's shares that day.[378] Hindenburg's accusations included reports that Block "embraced predatory offerings and compliance worst practices to fuel growth and profit from facilitation of fraud against consumers and the government."[379] Yet Circle has also marketed its coins as a foundation for shrinking the "racial wealth gap."[380] In one way or another, nearly all wal-

375. These practices are age-old. For one of countless earlier examples of financial inclusion arguments for deposit brokerage, see Leslie Eaton, *A Shaky Pillar in Harlem; Black-Owned Carver Bank Seeks Solid Financial Base*, N.Y. TIMES (July 11, 1999), https://www.nytimes.com/1999/07/11/nyregion/a-shaky-pillar-in-harlem-black-owned-carver-bank-seeks-solid-financial-base.html (arguing the reluctance of banks to take advantage of new technology and regulatory arbitrage has hampered Black-owned banks).

376. "Predatory inclusion" seems to have been introduced in 2017 by the sociologists Louise Seamster and Raphaël Charron-Chenier in their analysis of racial inequalities in student loan markets. Louise Seamster & Raphaël Charron-Chenier, *Predatory Inclusion and Education Debt: Rethinking the Racial Wealth Gap*, 4 SOC. CURRENTS 199 (2017). For another use of the term, see Fair Housing Act, 42 U.S.C. § 3601 *et seq*.; Keeanga Yamahatta-Taylor, *How Real Estate Segregated America*, 65 DISSENT 23 (2018); KEEANGA YAMAHATTA-TAYLOR, RACE FOR PROFIT (2020). For use of a similar term "exploitative inclusion," see Gary Dymski et al., *Race, Gender, Power, and the US Subprime Mortgage and Foreclosure Crisis: A Meso Analysis*, 19 FEMINIST ECON. 124 (2013).

377. See Anderson, *supra* note 12.

378. Robert Devore, *Block: How Inflated User Metrics and "Frictionless" Fraud Facilitation Enabled Insiders To Cash Out Over $1 Billion*, HINDENBURG RSCH. (Mar. 23, 2023), https://hindenburgresearch.com/block [https://perma.cc/2J4L-H2F7].

379. *Id.*

380. *Id.*

let companies claim to "bank" the "underbanked" and "unbanked," although their products do not accomplish this task (see Part II). In addition to taking advantage of a general trust as a transmitter of funds, Plaid benefits from the practices of its business partners in fostering unique relationships with certain classes of consumers.

If the Bureau enhances its current approach to 1033 as suggested, its CBA for the rule as a whole will change. I do not engage in a whole 1022(b)(2) analysis. Dodd-Frank charges the Bureau to "consider" rather than "compare," "analyze," or "assess" costs and benefits but suggests no method for consideration. The statute does not require measurement or quantitative analysis.[381] It offers no guidance on considering costs versus costs, benefits versus benefits, or costs versus benefits. Dodd-Frank does not indicate how to consider costs and benefits when consumers and businesses have conflicting interests.

However, per the points I have made concerning the unfairness CBA requirement, I maintain that consumers can benefit from basic platform money services without the current data governance risks. In an immediate sense, my proposal is quite targeted. Data brokers could not conduct specific business activities in a specific market involving specific instruments and devices. Outside of the balance transfer context, data brokers would still be able to collect, use, and retain data according to the CFPB's "reasonably necessary" standard. For instance, Plaid could still use its databanks to offer underwriting services, but it would not be able to use the transaction data collected through commonplace Wells Fargo-Venmo balance transfers to do so. Plaid would have to rely on data collected through other contexts.

The broader impact on other components of the open banking sector is less clear, in part because regulators and the public know so little about how brokers actually share data throughout the fintech ecosystem. The relative impact of my proposal hinges on how much, for instance, fintech companies partnering with Plaid rely on the data that Plaid collects from balance transfers as opposed to data it collects in other contexts. Some digital wallet companies, such as Venmo, offer credit cards and in doing so, assess the transaction data it receives from Plaid. Venmo could still offer credit cards. Yet, Venmo would have to obtain data from Plaid (or another broker, bank, or consumer reporting agency) outside the balance transfer context.

The rule would be less likely to directly impact companies outside the Platform Money ecosystem. For instance, the enhanced data minimization standard would not directly impact how SoFi and Plaid could col-

381. The courts do not impose a duty to quantify or net costs and benefits if Congress has not explicitly created such a duty in the statute. *See, e.g.*, Am. Textile Mfrs. Inst., Inc. v. Donovan, 452 U.S. 490, 510-12 & 510 n.30 (1981).

lect, use, or process data for lending because there is no balance transfer involved. SoFi does not store value. Plaid would still share data between banks and SoFi according to the CFPB's general Open Banking Rule requirements and data minimization standard. That said, if SoFi were to avail itself of Plaid's data to score a consumer or underwrite a loan, it would not be permitted to use data Plaid had collected in the simple balance transfer context.

The Rule would inevitably entail real tradeoffs. At the moment, however, policymakers are in a rush to pass the Open Banking Rule without adequately discussing these tradeoffs. In particular, policymakers risk entrenching the path dependency of data maximization. I suggest a more nuanced approach toward innovation that does not center acceleration. While focusing on the benefits of lowering switching costs and increased competition for individuals, we should be careful not to foreclose future policy frameworks or enable broader social harms.

VI. Public Governance

As one tech journalist puts it, Plaid now acts, "[l]ike a canal on a major trade route, it sits at a key point between users and their banks, observing and directing flows of personal information both into and out of the financial system."[382] Plaid characterizes its services as providing the pipes between fintech companies and traditional financial institutions. This language rightfully suggests Plaid serves a quasi-public function within the open banking sector.

As Lina Khan argues, when policymakers encourage monopolistic or anticompetitive market structures, there are at least two approaches.[383] Policymakers can focus on fostering competition or accept that they are inherently monopolistic or oligopolistic and adopt regulations to take advantage of these economies of scale while neutralizing the firm's ability to exploit its dominance.[384]

Under Director Rohit Chopra, the CFPB's policy orientation often promotes competition and mirrors the FTC's stance. I argue the CFPB should move closer to the regulated industries approach. The CFPB has adopted some public utility goals, particularly regarding "access and service rules" and familiar themes of horizontal competition, decentraliza-

382. *See* Bennett Cyphers, *Visa Wants to Buy Plaid, and With It, Transaction Data for Millions of People*, ELEC. FRONTIER FOUND. (Nov. 25, 2020), https://www.eff.org/deeplinks/2020/11/visa-wants-buy-plaid-and-it-transaction-data-millions-people [https://perma.cc/B2KP-3XH2].

383. Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 790 (2017).

384. *Id. See also* RICKS ET AL., *supra* note 49, at 1 (arguing that whereas antitrust law is supposed to safeguard the competitive process, NPU law is focused on areas in which regulation has been found necessary to compensate for the inability of competition to provide adequate regulation).

tion, access, and interoperability. In doing so, it mirrors policy approaches of the Federal Communications Commission (FCC). However, there are other important goals. The CFPB should move further along a continuum of public governance over critical networks, platforms, and utilities in regulated industries, which has long co-existed with anti-monopoly approaches.[385] In particular, within its mandate for holistic consumer financial protection, the CFPB should better balance its interest in competition with its interests in the stability of the banking system and data governance.[386]

Recently, a growing group of scholars has promoted a revival of the regulated industries tradition under the banner of "network, platform, and utilities law" (or "NPU Law").[387] Regulated industries law previously went under the banner of "the law of public utilities," "the law of public service corporations," and the "law of common carriers."[388]

During the Industrial Revolution in the United States, public utility regulation evolved from common law roots in the law of public callings, the police power, as well as legislative and public service corporate chartering.[389] Municipal governments were the first to regulate utilities in the nineteenth century through a franchise contract model.[390] The city would grant a utility company the necessary property rights—to build gas pipes, for example—and, in return, negotiate price caps to protect its citizen-consumers.[391] By the first decade of the twentieth century, many states created commissions, many enduring today.[392] The utility commissions aimed to provide the public with safe and adequate transportation, com-

385. Elettra Bietti, *A Genealogy of Digital Platform Regulation*, 7 GEO. L. TECH. REV. 1, 59-62 (2023).

386. Fortunately, scholars have recently generated a wave of new literature at the intersection of banking and antitrust. *See, e.g.*, Saule T. Omarova & Graham S. Steele, *Banking and Antitrust*, 133 YALE L.J. 1162 (2024) (arguing that contrary to the prevailing view, U.S. bank regulation operates as a comprehensive antimonopoly regime, designed to prevent excessive concentration of private power over the supply and allocation of money and credit in a democratic economy). *See also id.* at 1249-50 (arguing the "growing specter of Big Tech becoming an integral part of the new-generation TBTF finance—bigger, faster, and relentlessly expansive—heightens and concretizes these concerns."); Kathryn Judge, *Brandeisian Banking*, 133 YALE L.J. F. 916, 918, 938-41 (2024) (responding to Omarova and Steele, providing a more expansive account of the historical context of banking reform and anti-monopoly efforts, while recognizing financial stability and promotion of competition can come into sharp conflict); Jeremy C. Kress, *Reviving Bank Antitrust*, 72 DUKE L.J. 519, 520 (2022) (proposing a roadmap for reviving bank antitrust by strengthening the analytical tools used to identify anti-competitive bank mergers and rejecting a narrow focus on consumer prices). *See also* Daniel Hawley, *Coordination Rights After Bank Failure*, COLUM. L. REV (forthcoming) (analyzing the relationship between banking resolution and antitrust principles).

387. RICKS ET AL., *supra* note 49 at 1.

388. *Id.*

389. Bietti, *supra* note 385, at 275.

390. White, *supra* note 75, at 1247-48.

391. *Id.* at 1248.

392. *Id.*

munication, and energy services at reasonable rates.[393] Typical regulations also included, for instance, minimum service level, quality assurance prescriptions, and a defined or capped rate of return on investments.[394]

However, public utility regulation is most closely associated with the 20th-century progressive movement and New Deal.[395] The federal government and the states have used single regulatory commissions for an industry, multiple commissions with different missions, public ownership, monopoly, oligopoly, and broadly competitive market structures. At times, legislatures and regulators have intervened to restructure markets by breaking up industries vertically (e.g., by separating power generation and distribution or local and long-distance telephone service) or horizontally (e.g., the AT&T breakup).

Scholars began to increasingly critique the public utility model during World War II, accelerating in the 1970s and gaining hegemony in the 1990s.[396] Some scholars have dismissed the public utility idea as an archaic form of regulatory overreach, creating conditions ripe for regulatory capture and industry rent-seeking, protectionism, and self-dealing, deploying their charters as a weapon against competition.[397]

In contrast, scholars like Sabeel Rahman argue that the public utility moment was, in fact, a tremendous success.[398] The policy movement catalyzed the creation of new administrative agencies at the state and local level and created a generation of lawyers and policymakers now skilled in these new legal tools and techniques, in effect setting up the creation of the modern administrative state and more practical, tailored governance.[399]

Today, policymakers and advocates return to public utility regulation as a methodology for re-imagining the governance of platform power. Much of the literature recognizes that companies offer immediate consumer benefits, including new services and low prices. But firms like Google and Amazon exercise increasing control over services that are themselves increasingly "infrastructural."[400] Public utility regulation shifts

393. *Id.*

394. Douglas Arner et al., *Governing Fintech 4.0: Bigtech, Platform Finance, and Sustainable Development*, 27 FORDHAM J. CORP. & FIN. L. 1, 63 (2022).

395. K. Sabeel Rahman, *Infrastructural Regulation and the New Utilities*, 35 YALE J. ON REGUL. 911, 916–25 (2018).

396. K. Sabeel Rahman, *Regulating Informational Infrastructure: Internet Platforms as the New Public Utilities*, 2 GEO. L. TECH. REV. 234, 238 (2018)

397. *See, e.g.*, Horace Gray, *The Passing of the Public Utility Concept*, 16 J. LAND & PUB. UTIL. ECON. 8 (1940).

398. Rahman, *supra* note 396, at 238-39.

399. *Id.*

400. Rahman, *supra* note 51, at 1626-27.

the focus from individual consumer welfare and economic efficiency to power relations between consumers and corporations.[401]

My proposal promotes three principles in the regulated industries tradition.[402] First, I maintain and support the Bureau's establishment of universal access and service requirements. Second, the proposal helps structurally separate—or "firewalls"—banking and commerce. Third, it encourages policymakers to shore up the regulated banking sector and supply "public fintech" infrastructure, as I have argued in other work.[403]

A. Access and Service Rules

The CFPB has drawn on specific methods of public utility regulation in the tech sector more so than the banking sector. In particular, the Bureau's approach to financial data governance more closely resembles the "net neutrality" effort in telecommunications regulations.[404]

Following years of allegations of unfair competition, Congress broke up AT&T in 1981, and the ensuing reform efforts culminated in the Telecommunications Act of 1996. Congress aimed to create competition between companies, requiring the unbundling of services offered to consumers but ensuring that all service providers were "interconnected"—that the basic infrastructure of telecom wiring was such that users of one provider could still call users of another provider.[405] In effect, this created a universal backbone infrastructure for telecommunications regulation, on top of which different companies would compete to offer services.[406] Net neutrality means internet service providers (Verizon, AT&T, Comcast, etc.) should treat all the data that travels over their networks equally and not discriminate in favor of particular apps, sites, or services.[407] Net neutrality prevents internet service providers from creating "fast lanes," censoring content, throttling traffic, and even outright blocking access to their competitor's products.[408] In 2015, during the Obama Administration, the FCC issued the Open Internet Order, establishing some net neutrality protections.[409] In 2017, during the Trump Administration, the FCC revoked the rule. On April 25, 2024, the FCC voted to restore the regula-

401. *Id.* at 1628-29.

402. *See, e.g.*, *id.* at 1626 (promoting firewalling, negative and positive public obligations, and public options).

403. *See generally* Carrillo, *supra* note 34.

404. Rahman, *supra* note 51, at 1650-57.

405. *Id.*

406. *Id.*

407. *Battle for the Net*, FIGHT FOR THE FUTURE, https://www.battleforthenet.com/?org=dp [https://perma.cc/T8XJ-VGRQ].

408. Rahman, *supra* note 51, at 1669.

409. *Id.* at 1650-57.

tions—a critical victory for the White House unified strategy to promote competition.[410]

The values of net neutrality are also important in the data transmission context of open banking. Indeed, NPU scholars point out that the National Banking Act of 1864 anticipates a nationally integrated system with interoperability and continuity of service.[411] However, like the promotion of competition, they represent only one set of considerations, which we should contextualize within broader objectives. As Julie Cohen warns in her critique of net neutrality, we should be careful not to "assume that market forces operating on an internet platform basis will produce services of adequate variety and quality as long as access providers are prevented from blocking or throttling such services."[412] In the platform money context, we should not assume that opening up data flow between banks and tech companies will necessarily improve outcomes for consumers.

B. Structural Separation

Many Progressive and New Deal regulators aimed to separate core necessities from business practices that might contaminate the essential provision of these goods and services, including structural limits on the corporate organization and form of firms that provide infrastructural goods.

The separation of banking from commerce has deep roots in banking law.[413] Historically, commercially-owned banks have made unsound loans to business partners, denied services to competitors, and generally engaged in imprudent activities to spur commercial user purchases.[414] Commercial firms that also engage in financial services tend to use such enterprises to fund other risky business activities, heightening the moral hazard of bailout.[415] The risk of predatory behavior increases.

As discussed in Part II, the platform money sector intentionally bridges banking and commerce. The CFPB's Open Banking Rule could make it easier for consumers to switch between banks and other financial institutions, which could make them less reliant on the nation's largest and most politically powerful banks, the big three credit reporting bu-

410. Cecilia Kang, *F.C.C. Votes to Restore Net Neutrality Rules*, N.Y. TIMES (Apr. 25, 2024), https://www.nytimes.com/2024/04/25/technology/fcc-net-neutrality-open-internet.html [https://perma.cc/D2Y3-56SK].

411. RICKS ET AL., *supra* note 49, at 13.

412. COHEN, *supra* note 30, at 176.

413. RICKS ET AL., *supra* note 49, at 29.

414. Arthur E. Wilmarth, Jr., *Wal-Mart and the Separation of Banking and Commerce*, 39 CONN. L. REV. 1539, 1598-1606 (2007).

415. *Id.* at 1569.

reaus, and Mastercard and Visa's duopoly over payment processing.[416] However, the data brokers could become too economically and politically powerful with respect to the banking system.

My proposal slows Plaid's pace, reducing the banking data it collects, uses, and retains by mere virtue of being a middleman.[417] Plaid is already entering markets that its clients serve—it could easily offer services closer to the heart of banking law.[418] It could enter the digital wallet business by partnering with banks and cutting out incumbents. Plaid could obtain an industrial loan charter or simply partner with a bank in a relatively unregulated state to enter the broader banking business, giving it some unrivaled power over consumers, governing both funds and data. In doing so, Plaid would likely enjoy a comparative advantage in these markets, given their control over the data ecosystem.

Awrey and Macey have suggested data aggregators should be prohibited from owning, controlling, being owned or controlled by, otherwise being affiliated with, or having a material economic interest in any firm directly operating within the regulated financial services industry.[419] In the short run, platform money challenges stodgy banks. In the long run, however, the economics of data aggregation point toward a highly concentrated data broker industry. This new market structure would effectively recreate the informational vaults that open banking champions seek to unlock.[420]

I agree policymakers should generally attempt to structurally separate banks and large tech companies, but platform money and data maximization undermine this effort. I have previously argued we need structural partitions between commerce and banking, and between major tech platforms and payment systems.[421]

---

416. Kevin Robillard, *The Obscure Biden Administration Rule That Could Help Americans Flee Big Banks*, HUFFPOST (Apr. 7, 2021), https://www.huffpost.com/entry/the-obscure-biden-administration-rule-that-could-help-americans-flee-big-banks_n_606e0dd0c5b6034a708417e9 [https://perma.cc/5NXA-QASC].

417. For more on the increasing power of intermediary actors in the economy, see generally KATHRYN JUDGE, DIRECT: THE RISE OF THE MIDDLEMAN ECONOMY AND THE POWER OF GOING TO THE SOURCE (2022).

418. This is a "platform envelopment" strategy, whereby a dominant platform operating in one market seeks to expand into a second platform market, ultimately with a view to offering bundled products and services. Awrey & Macey, *supra* note 2, at 57-58.

419. *Id.* at 56-58. *See also id.* at 52 (characterizing a CFPB licensing regime as a 'modest proposal' compared to federal legislation separating "data aggregation from finance").

420. *Id.* at 57.

421. *See License to Bank: Examining the Legal Framework Governing Who Can Lend and Process Payments in the Fintech Age: Hearing Before the Task Force on Financial Technology of the Committee on Financial Services* 23-24, 115th Cong. (2020) (testimony of Raúl Carrillo, Policy Counsel, Demand Progress Educ. Fund), https://www.congress.gov/116/meeting/house/111057/witnesses/HHRG-116-BA00-Wstate-CarrilloR-20200929.pdf [https://perma.cc/M69Y-ZLXB].

C. Public Infrastructure

For some scholars, the public utility regulation is but a waystation to public infrastructure, and often failed waystations at that.[422] They argue that by the postwar period, consumer protection quickly faded as a goal, and companies used public utility status to gain immunity from prosecution under the antitrust law.[423] Some scholars argue that the popularity of public utility among experts decreased support for public or cooperative production and distribution of electricity.[424]

From the perspective of scholars who argue banks are critical networks, platforms, and utilities, even public utilities,[425] the open banking industry exists because of failures of banking law and policymaking. If these flaws—slow payments, high fees, low interest on savings, lack of coverage, etc.—persist, Silicon Valley will continue to develop a layer on top of the system that ostensibly benefits consumers but unnecessarily risks significant harm. If everyone could make instant payments and funds transfers between bank accounts, there would be no need for Venmo, Cash App, and Plaid (and a minimized need for Circle).

The most vital parts of the CFPB's proposed rule explanation also point toward this approach. For instance, its discussion of increased standardization "benefit to third parties' betrays an analysis of the data brokers as dispensable middlemen in open banking. The CFPB expects uniform standards for data access to help decrease the cost of third parties accessing customer data to the point where it would allow some third parties to bypass data aggregators and connect directly with data providers like banks or even all.[426] This structural adjustment would further reduce data broker market power "because a direct connection with a data provider is a substitute for aggregator services; a decrease in the cost of direct connections would likely decrease the price of aggregator services."[427]

Ultimately, we should move toward the public provision of many financial services discussed in this Article. We are inviting Silicon Valley and Wall Street to collaborate on infrastructure that should be public in the first place. Agencies in the United States have long created state-

422. Gray, *supra* note 397, at 9("The public utility concept retained and reaffirmed the basic fallacy of the late nineteenth century-namely, that private privilege can be reconciled with public interest by means of public regulation. True to the liberal tradition, it assumed a fundamental harmony between private and public interest; this being the case, specific instances of conflict were regarded as temporary aberrations or maladjustments which in no wise vitiated the general rule.").

423. *Id.* at 11.

424. *Id.* at 12.

425. *See supra* Part II.

426. Proposed Open Banking Rule, *supra* note 3.

427. *Id.* at 74857.

licensed, cheaper, basic versions of critical services to offer an alternative to exploitative private control in markets otherwise immune to competitive pressures.

Other governments worldwide have provided public infrastructure for real-time (nearly instantaneous) payments. Some have been active since the early 2000s, and others (in Asia especially) have been active since the 1970s and 1980s. In the United States, the private sector developed a real-time payment option—The Clearing House RTP., owned by banks in consortium—in 2017. However, the Federal Reserve System did not offer similar infrastructure until it launched "FedNow" on July 20, 2023. FedNow allows financial institutions to let customers make payments that can be sent at any time and received within seconds, with funds immediately available. It is available to depository institutions in the United States and enables individuals and businesses to send instant payments through their depository institution accounts.[428] But banks must opt-in and have thus far been hesitant to do so.

The Fed has clarified it does not intend for FedNow to replace Venmo or Cash App, as FedNow does not store value. Instead, it is meant to work alongside the current systems built by the private sector.[429] However, some banks already using the Fed's current, slower payment system may see FedNow as a safe and faster option with government backing. Zelle is the only app-based payment system that operates within the RTP network. The RTP Network's financial institutions can also opt into the FedNow system.

On a broader level, I have joined other reformers to support "public fintech" infrastructure, such as 'FedNow,' as well as public bank accounts, long-distance money transfers, and digital cash,[430] obviating the need for the most dangerous forms of platform money. Here, we must also center on innovative data governance ideas, such as tiered access to data and data trusts.[431]

428. *FedNow® Service*, BD. OF GOVERNORS OF THE FED. RSRV. SERV. (July 20, 2023), https://www.federalreserve.gov/paymentsystems/fednow_about.htm [https://perma.cc/CTG2-VR7B].

429. Rachel Witkowski, *FedNow FAQs: What The Fed's New Instant Payments System Is—And Is Not*, FORBES (July 20, 2023), https://www.forbes.com/advisor/personal-finance/fednow-faqs [https://perma.cc/UC9P-47S3].

430. Carrillo, *supra* note 34, at 1278-99.

431. Government agencies storing consumer data could establish institutions such as independent "public trusts" as stewards of that data. *See, e.g.*, Aziz Z. Huq, *The Public Trust in Data*, 110 GEO. L.J. 333, 333-34 (2021) (offering a "proof of concept" for how personal data economies can be leashed through the public trust form—a mechanism for minimizing private harms while preventing abusive state action).

VII. Conclusion

We are at a crossroads for the future of financial services. While many scholars and policymakers advocate for the use of new data-intensive technologies to promote competition and individual consumer control, we also risk ushering in an unsound data governance paradigm. In this Article, I have analyzed the CFPB's current approach toward "platform money"—billions of dollars of consumer funds stored by technology companies in digital wallets, unprotected by FDIC insurance or broader consumer banking regulation. Building on banking law concerns, I argue that platform money threatens systematic, social informational harms. As one critical, initial policy measure for consumer protection, the CFPB should apply an enhanced data minimization standard to brokers transferring balances between regulated banks and digital wallets, preventing brokers from collecting more data than is "strictly necessary" to transfer funds in compliance with existing laws. Overall, I echo the call for a revitalized approach to financial regulation promoting a continuum of public governance over critical networks, platforms, and utilities rather than competition per se.