**Testimony before the**

**U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON FINANCIAL SERVICES**
**Task Force on Financial Technology**

Regarding

"What's in Your Digital Wallet?
A Review of Recent Trends in Mobile Banking and Payments"

April 28, 2022

**Raúl Carrillo, Esq.**
**Associate Research Scholar, Yale Law School**
**Deputy Director, Law and Political Economy Project**

**Background & Summary**

Chair Lynch, Ranking Member Davidson, distinguished Members of the Task Force, thank you for inviting me to testify. I offer my testimony as an Associate Research Scholar at Yale Law School. I am also the Deputy Director of the Law and Political Economy Project.[1] I previously served as Special Counsel to the Enforcement Director of the Consumer Financial Protection Bureau (CFPB).

After roughly a decade of growth, the financial technology "fintech" industry is defined not so much by entrepreneurialism, but an arms race between major players on Wall Street and in Silicon Valley, who dramatically make and break alliances, and generally jockey for economic and political power. My previous remarks before this task force have called for policymakers to consider the deeper impacts of these dynamics on our society and principles of democracy. Today, I repeat the call for policymakers to adopt a bright-line, precautionary approach to technological developments involving financial products, sectors, and systems.

Sometimes it is easy to place new financial products and services into existing regulatory categories. It is more difficult when "fintech" or "techfin" products and services rely on the business model of Big Tech, namely *"data maximization"* -- the constant, expansive accumulation and analysis of consumer data.[2] New financial technologies like digital wallets may generate helpful information, serving as gateways to savings, credit, and investment. Yet based on their business models, they can also evade critical regulations, enabling new fines, fees, controls, algorithmic discrimination, and potentially, financial instability. Moreover, these new services and products operate within massive information networks, including consumer reporting agencies, specialty screen agencies, data brokers, and government agencies, which amplify systemic security and privacy risks, potentially creating a financial data collection ecosystem that is also "too big to fail." The risks of harm are especially pronounced for low-income communities of color that already suffer from financial injustices and privacy violations disproportionately.

Perhaps most importantly for the purposes of this hearing, digital wallet companies avoid banking regulation, even when consumers believe their funds are sufficiently protected, and even when the wallet providers perform the functions of legacy banking in concert with other companies. Moreover, wallet providers easily avoid privacy and data governance regulations crafted before contemporary data aggregation and predictive analytics.

As it stands, the CFPB has the widest regulatory powers for regulating the digital wallet space, and UDAAP rulemaking offers one alternative route to substantive, preventative regulation that can achieve some of the goals of banking and privacy laws, as well as

---

[1] "The Law and Political Economy (LPE) Project brings together a network of scholars, practitioners, and students working to develop innovative intellectual, pedagogical, and political interventions to advance the study of political economy and law." https://lpeproject.org/.

[2] *See, e.g.,* Omri Ben-Shahar, *Data Pollution*, 11 J. Legal Analysis 104, 140 (2019) (arguing that in the current legal regime, there is no reason for firms to scale their data activity to the perceived benefits, and no reason to stop short of "data maximization"--of collecting all possible information.); Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 Nw. J. Tech. & Intell. Prop. 239, 242 (2013) (arguing big data is premised on data maximization--a theory that posits that the more data processed, the finer the conclusions--and seeks to uncover surprising, unanticipated correlations).

independent goals.[3] Ultimately, however, Congress should also pass legislation bringing digital wallets further into the ambit of existing banking and financial services regulation, as well as legislation instantiating *data minimization,* including by limiting the collecting and processing of data to only that which is required to carry out an explicit, narrow purpose.[4] Most importantly, Congress can create public options that can both serve the country of their own accord and help to regulate the fintech space.

Today, I will make five overarching recommendations. Congress should:

- **Clarify rules regarding fraud, error resolution, and other fundamental consumer protections**
- **Designate deposit-like obligations as deposits, triggering banking (and bank holding) regulation**
- **Pass comprehensive data minimization legislation**
- **Work to create and maintain structural barriers between finance and commerce**
- **Establish inclusive, privacy-respecting public options for payments and financial services**

**Fraud & Error Resolution**

First, I echo the following recommendations recently submitted to the Consumer Financial Protection Bureau (CFPB) by a 65-member coalition of consumer and public interest advocates.[5] Congress or the CFPB should take the following actions:

- Clarify that all payment services providers and financial institutions have an existing duty under the Electronic Fund Transfer Act (EFTA) to investigate and resolve all errors committed through p2p systems, including errors committed by consumers.

- Enact a rule to define fraud in the inducement as an error covered by the EFTA's error resolution procedures.

- Most urgently, without waiting for an EFTA rulemaking to be complete, work with the Federal Reserve Board (FRB) to revise the proposed regulations for the soon-to-be-launched FedNow payment system to require financial institutions to protect consumers in the event of consumer errors or fraud in the inducement.

---

[3] For more on this idea, see Comment from Raúl Carrillo, Rohan Grey, and Luke Herrine to CFPB (Dec. 21, 2021), https://www.regulations.gov/comment/CFPB-2021-0017-0092.

[4] Data minimization means that only those data are processed (collected, stored, mined, inferenced, used for training algorithms) that are necessary. Mireille Hildebrandt, *Primitives of Legal Protection in the Era of Data-Driven Platforms*, 2 Geo. L. Tech. Rev. 252, 267 (2018).

[5] See Comment from National Consumer Law Ctr. et al to CFPB (Dec. 21, 2021), https://www.consumeradvocates.org/wp-content/uploads/2022/01/Comment_CFPBTechPayments_12.2021.pdf. *See also* "H.R. ____, the "Protecting Consumers From Payment Scams Act," https://financialservices.house.gov/uploadedfiles/bills-117pih-protectingconsumersfrompaym-u1.pdf (updating the Electronic Fund Transfer Act to close gaps and clarify ambiguities when consumers are defrauded into sending money by covered payment apps).

- Clarify the protections when a consumer's account is wrongfully frozen, generally applying the EFTA's error resolution framework.

**Deposit Designation & Banking Regulation**

Most digital wallets do not simply transfer funds, but store balances unprotected by federal deposit insurance or any equivalent mechanism.[6] By avoiding custody agreements with FDIC-insured institutions, many tech, fintech, and techfin companies avoid banking regulation, thereby functioning as *"shadow payment platforms*."[7] Consumers rarely understand that in the event of disaster, the last line of defense is general corporate bankruptcy law.[8]

I am particularly concerned with deceptive claims with respect to redemption in the stablecoin industry.[9] My concerns only intensify as digital wallets trend toward "super apps" -- one-stop shops for financial services -- as well as increased embednesess within the "Internet of Things" (smart transit terminals, wearables, cars, refrigerators, etc.).[10]

Congress should designate the deposit-like obligations of dominant tech platforms as "deposits", prohibiting the platforms from issuing such obligations absent review and approval by banking regulators. We need a forward-looking bill that seeks to integrate emerging digital financial technologies into traditional banking services in a way that strengthens regulatory supervision, clarifies the legal status and classification of digital financial assets, but above all, promotes safety of consumer funds. We should recognize as a deposit any digital financial asset that promises a fixed nominal value, on demand, denominated in or pegged to the U.S. dollar, and regulates the relevant institutions as depository institutions. I believe the recent White House memorandum on stablecoins makes significant strides in this direction,[11] but the STABLE Act recently proposed by Rep. Rashida Tlaib (D-MI) achieves these goals more comprehensively.[12]

Policymakers may create a narrower space for firms that do not seek to engage in broader depository activities beyond accepting funds and making payments, but all companies must be subject to regulation that matches the risks posed to consumers and the broader public. Advocates and scholars across the political spectrum have argued our existing banking charter

---

[6] *See, e.g,* Sarah Jane Hughes & Stephen T. Middlebrook, *Advancing A Framework for Regulating Cryptocurrency Payments Intermediaries*, 32 YALE J. ON REG., 495, 527 (2015).

[7] *See* Dan Awrey & Kristin van Zwieten, *Mapping The Shadow Payment System* 41-44 (SWIFT Institute Working Paper No. 2019-00, 2019), available at: https://ssrn.com/abstract=3462351 (discussing comparative approaches in the U.S., UK, EU, and China).

[8] *See* Dan Awrey, *Bad Money,* 106 Cornell L. Rev. 1 (2020) (discussing how the corporate bankruptcy regime fails depositors).

[9] *See* the STABLE Act, which proposes to regulate stablecoins as bank deposits. Press Release, Tlaib, García and Lynch Introduce Legislation Protecting Consumers from Cryptocurrency-Related Financial Threats (Dec. 2, 2020), https://tlaib.house.gov/media/press-releases/tlaib-garcia-and-lynch-stableact; https://tlaib.house.gov/sites/tlaib.house.gov/files/STABLEAct.pdf

[10] "Ten years ago, tech investor Marc Andreessen famously proclaimed "software is eating the world" … now payments are eating the world." JPMORGAN CHASE, PAYMENTS ARE EATING THE WORLD 4 (2021), https://www.jpmorgan.com/solutions/treasury-payments/payments-are-eating-the-world

[11] President's Working Group on Financial Markets, FDIC, and OCC, Report on Stablecoins (Nov. 2021), https://financialservices.house.gov/uploadedfiles/hhrg-117-ba00-20220208-sd002.pdf

[12] See STABLE Act, *supra* note 9.

system is broken.[13] I have testified to the charter issue previously, so herein merely note that any attempt at creating new banking charters, or narrower payment charters, must, at the very minimum, provide a basis for the more comprehensive regulation of minimum balances or maximum balances, quantitative and qualitative regulation of fees, and privacy, security, and data governance policies.[14] In no scenario should we allow the regulations that flow from federal chartering to supersede or supplant any other stronger regulations or standards promulgated by other Federal or applicable State regulatory entities, including any such regulation issued by the FDIC or CFPB.

**Data Minimization**

As a structural matter, there are two key differences between the financial products of yesterday and today: the volume of data extracted by each participant, and the multiplication of participants, in the service chain.[15] While a traditional credit card payment implicates a merchant, two banks and a payments processor, a payment made with a mobile wallet includes those parties and a mobile device maker, telecom or internet service provider, and often, but not always, a consumer-facing service provider that creates and manages the app that facilitates the payment.[16]

Each of the many entities involved may collect and share consumer data with other companies. Mass financial surveillance eventually creates a detailed picture of our most private social, familial, romantic, religious, and political activities, offering a "picture of the person behind the payment."[17]

Supporters of ideas like "open banking" are right that helpful data is underproduced and inequitably inaccessible to consumers given the centrality of reporting and scoring in our economy. Concern for consumer control also aligns with worries that big banks have monopolized data that could improve the profiles of consumers. Economists have argued for potential advantages to credit data sharing, including: increased competition in financial services markets; additional visibility, transparency, and completeness with respect to data dossiers; more efficient pricing of credit, debt management, and collection.[18] U.S.

---

[13] *See* Dan Awrey, Unbundling Banking, Money, and Payments (January 31, 2021). European Corporate Governance Institute - Law Working Paper No. 565/2021, Available at SSRN: https://ssrn.com/abstract=3776739 or http://dx.doi.org/10.2139/ssrn.3776739.

[14] *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*, 116th Cong. (Statement of Raúl Carrillo, Policy Counsel, Demand Progress Ed. Fund & Fellow, Americans for Financial Reform Ed. Fund), https://www.congress.gov/116/meeting/house/111057/witnesses/HHRG-116-BA00-Wstate-CarrilloR-20200929.pdf.

[15] Consumer Reports, Comments to the CFPB in Response to the ANPR Regarding Consumer Access to Financial Records Under Section 1033 of the Dodd-Frank Act, Feb. 4, 2021. https://www.regulations.gov/comment/CFPB-2020-0034-0051

[16] For detailed discussion of these chains, see, e.g., Adam J. Levitin, *Pandora's Digital Box: The Promise and Perils of Digital Wallets*, 166 U. Pa. L. Rev. 305 (2018).

[17] Albert Fox Cahn & Melissa Giddings, *In the Age of COVID-19, the Credit Card Knows All*, Surveillance Technology Oversight Project - Urban Justice Center (May 18, 2010), https://www.stopspying.org/latest-news/2020/5/18/in-the-age-of-covid-19-the-credit-card-knows-all.

[18] Leon Yehuda Anidjar, Inbar Mizrahi-Borohovich, *Reinventing Credit Data Sharing Regulation*, 29 S. Cal. Interdisc. L.J. 177, 181–83 (2020).

administrative agencies may also use financial data collection in the public interest.

However, under the current regime, harmful data is also overproduced. In many instances, financial service providers reserve broad rights to use consumer data for unrelated purposes. Indeed, as recent hearings concerning Dodd-Frank Rule 1033 made clear, the fintech industry -- very much including digital wallet providers -- relies on the data broker industry, which adds payments and credit data to data stocks regarding employment, marital status, homeownership status, medical conditions, and even our interests and hobbies, especially as articulated via social media.[19] Frequently, the data aggregator stores the login credentials of consumers and uses them to continually log into the consumer's bank account to copy all personally identifiable data, ranging from transaction information to account numbers. Once it has accessed consumer data, the data aggregator can share or sell that data without the consumer's knowledge, much less consent.[20] Yet nearly 7 in 10 Americans think companies use personal data in ways they're comfortable with — about the same number who admit they never or only sometimes read privacy policies.[21]

No overarching federal privacy law currently curbs the collection, use, and sale of personal data among corporations.[22] At this point, leading scholars of data governance of varying intellectual and political perspectives have concluded that laws on the books, including financial privacy laws, do not sufficiently protect consumers in the era of predictive analytics.[23] Definitionally, notice-and-consent laws cannot empower people to protect their privacy because, when people "consent" to share data, they do not know what they are really agreeing to reveal or to what end, how long the information will be stored, the probability of eventual errors, etc. When we generate data, we cannot fully predict how they may help or harm others.[24]

Individual rights alone cannot account for the collective harms of datafication the flow within the financial system and beyond it. Financial data governance requires balancing the necessity of collecting highly personal and consequential information and the risk of harm that accompanies its processing. This is especially important as we consider practices of "financial inclusion."

---

[19] HFSC, Preserving the Right of Consumers to Access Personal Financial Data, 117 th Cong. (Sept. 21, 2021).

[20] Even though they are not new entities, companies like Plaid, Intuit, Finicity, Envestnet|Yodlee, Morningstar/ByAllAccounts, Fiserv/CashEdge, and MX are "barely subject to any regulation, have received little scholarly attention, and most consumers have never even heard of them or know what they do." For timely legal analysis of data aggregators' relationships with banks, tech companies, and consumers in the context of Section 1033, see generally, Nizan Geslevich Packin, *Show Me the (Data About the) Money!*, 2020 Utah L. Rev. 1277 (2020).

[21] Erica Turner, *Americans attitudes and experiences with privacy policies and laws*, Pew Research Center (Nov. 15, 2019), www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/.

[22] Berkeley Media Studies Group et al., The Time is Now: A Framework for comprehensive privacy protection and digital rights in the united states, Citizen.org, (last visited Mar. 31, 2020), https://www.citizen.org/sites/default/files/privacy-and-digital-rights-for-all-framework.pdf

[23] For an extensive list of the most prominent visions of a new regulatory paradigm, see 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, 446–47 (2020).

[24] For a general theory of data governance and democracy strongly informing this testimony, *see* Salomé Viljoen, *A Relational Theory of Data Governance*, 131 Yale L.J. 573 (2021).

Most fintech business models rely on data maximization that renders marginalized communities more vulnerable. By law, financial data is increasingly co-monitored by law enforcement via mass, pre-emptive, predictive, and perpetual surveillance.[25] Poverty, family, criminal, immigration, and national security law have already made mass financial surveillance a channel for policing troubled by civil rights concerns. In perhaps its most dangerous instantiation, many fintech enterprises,[26] including wallet providers, are attempting to create a biometric "decentralized and portable digital identity" to substitute for government ID or functionally become the government ID in some places.[27] Many of these proposals involve biometric tools like facial recognition technology (FRT), iris-scanning, and palm prints, which are vehemently opposed by many privacy advocates, who argue this data is easily obtainable by law enforcement agencies.[28] This dimension of "financial inclusion" is understudied and often ignored in policy debate.[29]

Ultimately, Congress must shift the burden of data protection from consumer, courts, and litigators, to regulators and technology companies. The collision and collusion of Big Tech and Wall Street in this space demands especially careful scrutiny. Companies, whether fintech, techfins, or any other permutation, should not be collecting any data that is not strictly necessary for the provision of a good or service. For example, signing up for a credit card online should not lead to targeted advertising (or new accounts). We should not be able to forfeit our rights to data privacy and security, in particular, simply by clicking "I agree", or providing token consent to data usage policies consumers do not understand and firms cannot and do not uphold.

Congress should pass law that would restrict data collection, processing, storage, and sharing to a narrow list of permissible purposes and prohibit various forms of data-driven discrimination. The law should also establish concrete fairness requirements that must be satisfied including operating requirements; adherence to standard protocols; subjection to supervisory examinations, including the supervision the testing of automated decision systems; public transparency obligations with respect to business data collection; and finally, strong

---

[25] For discussion of the public-private nature of surveillance and its relationship to regulation, informing this testimony, see Julie E Cohen, *How (Not) to Write a Privacy Law*, Knight First Amendment Institute (Mar. 23, 2021), knightcolumbia.org/content/how-not-to-write-a-privacy-law.

[26] Leon Perlman & Nora Gurung, Focus Note: The Use of eKYC for Customer Identity and Verification and AML 8 (May 14, 2019), *available at* https://ssrn.com/abstract=3370665 (last visited June 22, 2020).

[27] S*ee* Ian Allison, *How Anti-Money-Laundering Rules Hinder Libra's Mission to Reach the Unbanked*, CoinDesk (Oct. 9, 2019), https://www.coindesk.com/how-anti-money-laundering-rules-hinder-libras-mission-to-reach-the-unbanked.; ET Bureau, *Aadhaar verdict: Telcos, banks & financial companies may feel the pinch*, The Econ. Times (Sept. 27, 2018), https://economictimes.indiatimes.com/news/politics-and-nation/aadhaar-verdict-telcos-banks-financial-companies-may-feel-the-pinch/articleshow/65973414.cms.

[28] Facial recognition software is likely to mislabel or misrecognize members of racial minority groups, especially Black Americans. *See, e.g.,* Victoria Burton-Harris & Philip Mayor, *Wrongfully Arrested Because Face Recognition Can't Tell Black People Apart*, ACLU (June 24, 2020), https://www.aclu.org/news/privacy-technology/wrongfully-arrestedbecause. However, many civil rights advocates argue that the incompleteness of FRT databases is a good thing. Zoé Samudzi, "Bots Are Terrible at Recognizing Black Faces. Let's Keep It that Way," *Daily Beast*, February 8, 2019, https://www.thedailybeast.com/bots-are-terrible-at-recognizing-black-faces-lets-keep-it-that-way.

[29] *See* Carrillo, *supra* note 14.

sanctions against violators, including not only decrees and fines, but disgorgement and personal liability for senior executives and board members.[30]

Sen. Sherrod Brown's Data Accountability and Transparency (DATA) Act, released in discussion draft form in 2020, would prohibit most collection and sharing of personal data as its starting point.[31] Data could only be used in ways stipulated in the law, wherein collection is limited to permissible purposes, such as providing a service a consumer asked for — and no more. Not permitted: using data for alternate purposes, holding onto it longer than necessary to carry out the original purpose, or sharing it unless that's needed for the original purpose. In a boon to security concerns, personal data would not be retainable beyond a period of time *strictly necessary* to carry out a permissible purpose. DATA 2020 would als explicitly ban the use of facial recognition technology and prohibits the use of personal data to discriminate in housing, employment, credit, insurance, and public accommodations

This approach appropriately shifts the burden of privacy protection away from consumers, who have minimal resources to protect themselves, and toward corporations, which profit immensely from the aggregation of our data.

**Separating Commerce & Finance**

Recently, antitrust advocates have argued for open banking and sharing of data between apps, data sharing appears to cut against the trend in the industry towards data privacy. However, if not approached thoughtfully, regulatory history demonstrates that open access and interoperability requirements can actually serve as instruments by which dominant firms obtain and entrench monopoly power.[32]

The encroachment of new data collection business models into financial services may in some instances grant too much power to monopolistic firms. Dominant platforms grow by expanding their platforms' user base and information access, securing revenue by selling products directly to their users or by selling access to their users to third parties.[33] As U.S. legal scholars and European antitrust authorities have concluded, data begets market power, but market power also allows dominant platforms to continually extract data in unfair ways.[34] For instance, Amazon already provides the cloud-computing systems that serve as the "technological backbone" of many fintech firms, which grants Amazon access to data other companies are structurally unable to obtain.[35] The company could easily take advantage of this data to unfairly

---

[30] *See* Cohen, *supra* note 25.
[31] *See* Press Release, Brown Releases Proposal to Protect Consumers Privacy, Jun. 18, 2020, *available at* https://www.brown.senate.gov/newsroom/press/release/brown-proposal-protect-consumers-privacy/.
[32] *See, e.g.,* Awrey, Dan and Macey, Joshua, *Open Access, Interoperability, and the DTCC's Unexpected Path to Monopoly* (July 12, 2021). Available at SSRN: https://ssrn.com/abstract=3885194 or http://dx.doi.org/10.2139/ssrn.3885194. ("Our paper tells the untold story of how the SEC's attempt to promote competition in US securities clearing and depository markets through mandated interoperability ultimately paved the way for the DTCC's current monopoly over these systemically important markets.")
[33] *See, e.g.*, Wilson C. Freeman & Jay B. Sykes, Cong. Research Serv., R49510, Antitrust and 'Big tech' (2019), https://fas.org/sgp/crs/misc/R45910.pdf.
[34] Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 Harv. L. Rev. 497, 518 (2019).
[35] John Detrixhe, *Amazon is invading finance without really trying*, Quartz (Nov. 1, 2017), https://qz.com/1116277/amazons-aws-cloud-business-is-reshaping-how-the-financial-services-industry-works/

compete with its existing fintech business partners. Similarly, much of the fear around the Facebook Diem system concerned the likelihood of Facebook taking advantage of the Diem platform to support its new digital wallet, Novi, in an unfair fashion, scaling its platform power to unprecedented levels.[36]

If approached carefully, with data minimization in mind, the CFPB's Section 1033 Rulemaking could give consumers control over their financial data, which should make it easier for them to switch between financial institutions, which could make them less reliant on the nation's largest and most politically powerful banks, the big three credit reporting bureaus, and Mastercard and Visa's duopoly over payment processing.[37]

Just as the CFPB opens the space for safe and fair competition, though, legislators should reestablish a bright line between the ownership of large tech companies and the ownership of financial institutions. We need structural partitions between commerce and banking, profit-driven enterprise and "money creation," and platforms and payment systems.[38] Even smaller tech and fintech companies are now acquiring regulated banks.[39]

**Public Options & Financial Inclusion**

Financial technology can provide great benefits to society, but only if shaped by policymakers' own forward thinking about services people need in an information economy. Policymakers must avoid being swayed by general promises of 'innovation' and create systems that are safe for and accountable to the public.

Like many colleagues, I support the creation of a Digital Dollar and digital public options for a wide array of financial services and products, including bank accounts for all.[40] However, the new public systems should also be attuned to concerns of data minimization. Accordingly, I strongly support the E-CASH Act proposed by Representative Lynch:[41]

*"The ECASH Act would establish a two-stage pilot program led by the U.S.*

---

[36] For analysis of the Diem project from the perspective of the laws of regulated industries, see RAÚL CARRILLO, BANKING ON SURVEILLANCE: THE LIBRA BLACK PAPER, AFR ED. FUND & DEMAND PROGRESS ED. FUND (2020), https://ourfinancialsecurity.org/wp-content/uploads/2020/06/Libra-Black-Paper-FINAL-2.pdf [hereinafter BLACK PAPER].

[37] Kevin Robillard, *The Obscure Biden Administration Rule That Could Help Americans Flee Big Banks*, HuffPost Latest News (Apr. 7, 2021), www.huffpost.com/entry/the-obscure-biden-administration-rule-that-could-help-americans-flee-big-banks_n_606e0dd0c5b6034a708417e9.

[38] *See* Letter from Ams. for Fin. Reform Ed. Fund and Demand Progress Ed. Fund to H. Comm. on the Judiciary (Apr. 17, 2020), https://ourfinancialsecurity.org/2020/04/joint-letter-promote-tradition-of-separating-banking-and-commerce-regarding-dominant-platforms/ (arguing for the structural separation of large tech platforms and payments).

[39] *See, e.g.*, Hugh Son, *LendingClub buys Radius Bank for $185 million in first fintech takeover of a regulated US bank,* CNBC (Feb. 18, 2020), https://www.cnbc.com/2020/02/18/lendingclub-buys-radius-bank-in-first-fintech-takeover-of-a-bank.html.

[40] *See, e.g., Digitizing the Dollar: Investigating the Technological Infrastructure, Privacy, and Financial Inclusion Implications of Central Bank Digital Currencies, Hearing Before the Task Force on Financial Technology of the Committee on Financial Services*, 116th Cong. (Statement of Rohan Grey, Ass't Prof., Univ. of Willamette College of Law), https://financialservices.house.gov/events/eventsingle.aspx?EventID=407953

[41] *Rep. Lynch Introduces Legislation to Develop Electronic Version of U.S. Dollar*, Congressman Stephen Lynch (Mar. 28, 2022), lynch.house.gov/press-releases.

*Department of the Treasury to develop and issue an electronic version of the U.S. Dollar that promotes consumer safety and privacy, financial inclusion and equity, and anti-money laundering and counterterrorism compliance. In order to maximize consumer protection and data privacy, the bill requires the Treasury to incorporate key security and functionality safeguards into e-cash that are generally associated with the use of physical currency – including anonymity, privacy, and minimal generation of data from transactions. In the interest of expanding financial inclusion, e-cash must also be interoperable with existing financial institution and payment provider systems, capable of executing peer-to-peer offline transactions, and distributed directly to the public via secured hardware devices. Moreover, the bill specifies that e-cash would be regulated similar to physical currency and subject to existing anti-money laundering, counterterrorism, Know Your Customer, and transaction reporting requirements and regulation."*

Although we have much to discuss and determine with respect to infrastructure, distribution, and other critical matters, public digital cash would serve the basic functions of payment, while avoiding many of the major issues discussed at this hearing. By functioning offline, e-cash wallets could be used by the one in three adults who lack high-speed internet access at home.[42] By operating via secured hardware rather than software, these 'minimalist' "low-tech" payment instruments would limit data collection and attendant privacy and security risks. If digital cash were to compete with digital wallet transactions, it could help regulate the unfair, unsafe, and undemocratic data collection that dominates our current financial system.

[42] 33% of adults lack high-speed internet access in their homes. Between 41% and 44% of adults in low-income communities lack high-speed internet access in their homes. Smartphones required for fintech outside the home are often prohibitively expensive. TERRI FRIEDLINE, BANKING ON A REVOLUTION 131-148 (2020).