epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

Federal Reserve

on

Money and Payments: The U.S. Dollar in the Age of Digital Transformation

May 20, 2022

The Electronic Privacy Information Center ("EPIC") submits these comments in response to the Federal Reserve's call for feedback on its January 2022 discussion paper: The U.S. Dollar in the Age of Digital Transformation.[1] The paper lays out pros and cons of implementing an intermediated central bank digital currency (CBDC) in the United States as a potential first step towards developing such a currency. In our view, the creation of an intermediated CBDC could improve financial privacy for individuals if the system is designed to facilitate anonymous transactions equivalent to cash and minimize the amount of data generated about individuals' purchases.

EPIC is a public interest research center in Washington, D.C. established in 1994 to focus on public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC has long advocated for robust safeguards to protect consumers from exploitative data collection, usage, distribution, and retention practices.[2] EPIC has played a leading

[1] Federal Reserve, *Money and Payments in the Age of Digital Transformation* (Jan. 2022), https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf.
[2] EPIC Comments on CFPB Inquiry Into Big Tech Payment Platforms, CFPB-2021-0017 (Dec. 2021), https://epic.org/documents/epic-comments-on-cfpb-inquiry-into-big-tech-payment-platforms/; Consumer Reports and EPIC, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness*

role in developing the authority of the FTC to address emerging privacy issues and to safeguard the privacy rights of consumers.[3] Recently, EPIC provided detailed comments on the impact of artificial intelligence on financial privacy.[4]

EPIC urges the Federal Reserve to take a careful approach to a central bank digital currency that prioritizes privacy and does not repeat or exacerbate the privacy invasions in the current digital payments system. A privacy-protective CBDC would require close regulation and testing of the underlying protocols, systems, and devices and should be designed as a cash-like digital currency using a token-based system without a persistent digital ledger.

I. The Federal Reserve should not implement a CBDC that replicates the substantial privacy harms in the current digital payment.

In response to Question 1. What additional potential benefits, policy considerations, or risks of a CBDC may exist that have not been raised in this paper?

The discussion paper does not adequately describe the privacy risks created by current third-party payment systems and thus does not adequately describe the necessary legal, regulatory, and technological architecture that would be necessary to establish a privacy-protective CBDC. The discussion paper does acknowledge that an intermediated digital currency would present similar privacy risks to the current payment system:

> **Consumer privacy:** A general-purpose CBDC would generate data about users' financial transactions in the same ways that commercial bank and nonbank money generates such data today. In the intermediated CBDC model that the Federal Reserve

Rulemaking (Jan. 26, 2022), available at: https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf; *see generally*, EPIC, Data Brokers, available at: https://epic.org/issues/consumer-privacy/data-brokers/.

[3] See EPIC, What the FTC Could Be Doing (But Isn't) To Protect Privacy: The FTC's Unused Authorities (June 2021), https://epic.org/privacy/consumer/EPIC-FTC-Unused-Authorities-Report-June2021.pdf.

[4] Comments of EPIC, *Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning*, Comptroller of the Currency et al. (Jul. 1, 2021), https://archive.epic.org/EPIC-Financial-Agencies-AI-July2021.pdf.

would consider, intermediaries would address privacy concerns by leveraging existing tools.[5]

But the discussion paper does not explain the invasive data collection that pervades the current payment ecosystem. At this moment when the Federal Reserve is researching and considering alternatives that could improve payment systems, the Board should take the opportunity to consider what legal, regulatory, and technological changes would actually improve financial privacy for individuals. The report should include a close review of current data collection and use practices in the banking, payment, and fintech sectors and recommend changes that would establish much needed privacy protections for individuals.

The current system for both physical point of sale and online payments is under-regulated and subjects individuals to voluminous financial surveillance. Credit cards, online transactions, and point-of-sale systems all have access to detailed records of individuals' financial transactions, and many of the entities operating these systems are either selling this personal data to brokers, or they act as brokers themselves. Currently, large data sets of credit and debit card transactions are available for purchase to almost anyone. A search on the bulk dataset aggregator Datarade returned 35 separate datasets offering individual credit or debit card transactions for sale, and 234 total data sets offering transaction data including bank-to-bank transactions, electronic payment transactions, and loyalty card data.[6] The widespread dissemination of this data poses substantial privacy risks because this type of transaction data is easy to de-anonymize. In 2015 a study found that metadata from just four transactions in a dataset was enough to identify the cardholder in 90% of cases.[7]

[5] *Money and Payments in the Age of Digital Transformation* supra note 1, at 19.
[6] Datarade, Best Transaction Datasets, https://datarade.ai/data-categories/transaction-data (last accessed May 17, 2022).
[7] John Bohannon, Credit card study blows holes in anonymity, Science (Jan. 30, 2015), https://www.science.org/doi/full/10.1126/science.347.6221.468.

Current payment systems are designed to enable data brokers to collect, aggregate, and sell consumer data, and we do not have legal or regulatory privacy protections to protect against abuse.

The widespread brokering of financial transaction data can cause substantial harms to individuals. Brokers that collect or purchase transaction data can use it to build detailed profiles of individuals that can reveal or be used to infer private information about them, including their political views, their religious beliefs, their reproductive and family choices, and their personal preferences and habits. These data can also be used to underpin consequential decisions about where an individual can work, live, or even what price or level of service they receive. This pervasive profiling forces individuals into a "scored society" that frequently operates as a black box where they do not have access to the most basic information on how they are evaluated. Secret algorithms can be used to determine the interest rates on mortgages and credit cards, raise consumers' interest rates, or deny people jobs. For more information on black box algorithms, see the work of Frank Pasquale.[8] And many times, algorithmic scoring does not create rational results. In one instance, a consumer found that his credit score suffered a forty-point hit simply because he requested accurate information about his mortgage.[9] For more information see: EPIC, Data Brokers, https://epic.org/issues/consumer-privacy/data-brokers/, and EPIC, Screening and Scoring, https://epic.org/issues/ai/screening-scoring/.

The widespread collection and use of transaction data also exacerbates risks of overbroad government surveillance. Law enforcement agencies have reportedly begun to purchase bulk data from brokers in ways that can sidestep constitutional and statutory privacy protections. For example, Immigrations and Customs Enforcement (ICE) uses transaction data from utility payments to

[8] *See*, Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information (2015), Frank Pasquale, New Laws of Robotics: Defending Human Expertise in the Age of AI (2020).
[9] Barry Ritholtz, *Where's the Note? Leads BAC to Ding Credit Score*, ritholtz.com (Dec. 14, 2010), https://ritholtz.com/2010/12/note-bac-credit-score/.

identify allegedly undocumented individuals for arrest and deportation, even when those individuals live in "sanctuary cities" that have opted not to provide information to the agency.[10] Some of the data used by ICE uses was collected by credit reporting agency Equifax from another data broker holding more than 400 million utility records.[11] Federal agencies have also had real-time access to credit card transaction data since at least 2010, creating risks of oversurveillance, wrongful arrest, and abuse.[12] Access to credit card data can be obtained without a warrant.

The current digital payments landscape is over-surveilled and under-regulated. Individuals are subject to private and corporate surveillance from payment services providers and data brokers. That data is used to monitor, evaluate, and score individuals through opaque algorithms, eliminating financial privacy and harming individuals' access to credit, housing, and jobs. Much of the same data is available to law enforcement with little oversight or protections against misuse. The Consumer Financial Protections Bureau is currently conducting an inquiry into data collection by big tech platforms that facilitate transactions including Google, Apple, Facebook, and Amazon.[13] The Fed should join the CFPB in studying invasive payment monitoring practices by big tech companies that collect transaction data. Central Bank Digital Currency should not replicate the current system.

[10] Georgetown Center on Privacy and Technology, American Dragnet, Data-Driven Deportation in the 21st Century (May 10, 2022), https://americandragnet.org/finding3.
[11] *Id*.
[12] Ryan Singel, Feds Warrantlessly Tracking Americans' Credit Cards in Real Time, Wired (Dec. 2, 2010), https://www.wired.com/2010/12/realtime/?utm_campaign=Feed%3A+wired%2Findex+%28Wired%3A+Index+3+%28Top+Stories+2%29%29&utm_medium=feed&utm_source=feedburner.
[13] *See*, Rohit Chopra, Statement Regarding the CFPB's Inquiry into Big Tech Payment Platforms, CFPB (Oct. 21, 2021), https://www.consumerfinance.gov/about-us/newsroom/statement-regarding-the-cfpbs-inquiry-into-big-tech-payment-platforms/, CFPB, Notice and Request for Comment, n.1 (Nov. 5, 2021), available at https://www.federalregister.gov/documents/2021/11/05/2021-24176/notice-and-request-for-comment-regarding-the-cfpbs-inquiry-into-big-tech-payment-platforms.

II. The Federal Reserve should not implement a CBDC unless strong financial privacy regulations are in place.

In response to Question 11. Are there additional ways to manage potential risks associated with CBDC that were not raised in this paper?

The discussion paper lays out many options for managing the potential risks associated with CBDCs. However, we believe that the paper does not adequately address the risks posed by intermediary and third-party implementation of digital wallets. Recent developments in the fintech and cryptocurrency ecosystem have shown that wallet services pose potentially substantial risks of data abuse, fraud, and other unfair practices if not adequately regulated. Malicious or improperly vetted wallet systems can exacerbate the problems of data aggregation, financial surveillance, and fraud. Implementing any new technology creates risks during the adoption period, when individuals are especially vulnerable to fraud and exploitation. And digital wallets pose unique risks because they expose individuals to commercial exploitation of personal transaction data as well as the risk of malicious third-party fraud, theft, or manipulation.

Without close review prior to deployment and constant scrutiny following adoption, the software and systems used to facilitate payments via CBDCs could cause more harm than good. Rampant thefts and fraud in digital assets including cryptocurrency and Non-Fungible Tokens (NFTs) demonstrate the risks to consumers in implementing new and unregulated financial technologies. Digital wallets are currently used in cryptocurrency marketplaces, and associated transactions like the sale of NFTs. A recent study from Chainalysis found that more than $3.2 billion in cryptocurrency was stolen in 2021, with the trend accelerating in 2022.[14]

While most of the largest thefts are accomplished by hacking cryptocurrency platforms, individuals are also widely vulnerable to fraud and theft. For example, in May 2022, hackers were

[14] Defi Hacks Are on the Rise, Chainalysis (Apr. 14, 2022), https://blog.chainalysis.com/reports/2022-defi-hacks/.

able to spread fraudulent links across several popular NFT Discord channels, triggering automatic transfer of NFTs from unwitting users' digital wallets.[15] These thefts take advantage of individuals unaware of how easily current digital wallets can be exploited. Expanding digital wallet use across the economy by adopting a CBDC will expose even more vulnerable individuals to potential thefts and fraud. Digital wallets then present serious security risks that need to be addressed before widespread adoption, especially if they are to hold CBDC funds.

Digital wallets will have access to sensitive information and digital transactions, which inherently create detailed records unless designed to avoid them. Wallets apps will have access to users' personal information, banking information, and unless regulated could easily access phone location information as well.[16] Because digital wallets will have to interact with both banks and point-of-sale devices, the wallet is a potential privacy vulnerability as the app could collect information on both sides of a transaction. Unscrupulous wallet developers will have a strong incentive to design wallets that maximize data collection and make that data available for sale to data brokers. And similar risks exist for point-of-sale systems, which will only provide transaction privacy if they are designed to do so.

New laws, regulations, and thorough product-testing are necessary to protect privacy for digital currency transactions. The Federal Reserve should investigate the current marketplace for digital wallets and provide recommendations for the legislation, regulation, and product testing

[15] Lorenzo Franceschi-Bicchierai, Hackers Compromise a String of NFT Discord Channels, Vice (May 18, 2022), https://www.vice.com/en/article/k7wmpy/hackers-compromise-a-string-of-nft-discord-channels.
[16] *See e.g.*, Jennifer Valentino-DeVries et al., Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret, N.Y. Times (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

necessary to protect consumers if digital wallets are widely adopted. The following principles are a starting point:

- **Data Minimization**: digital wallet providers should be prohibited from collecting any data that is not strictly necessary to make the digital wallet work;
    - **No Transaction Records**: digital wallet providers should not be permitted to create and maintain records of transactions conducted using the wallet;
    - **No Location Data**: digital wallets should not be permitted to collect or store location data or to transmit it off the device holding the wallet;
    - **No Data Exploitation**: digital wallet providers should not be permitted to sell or transfer data collected from wallet users;
- **Regulation**: Congress should designate one agency to implement regulations for digital wallets;
- **Product Testing**: Congress should mandate that either the National Institute of Standards and Technology or a designated regulatory agency perform rigorous product tests on all digital wallet apps to ensure that the apps conform with the above principles.

III. A token-based CBDC that facilitates private payments could address some of the privacy harms in the digital payments space.

In response to Question 12. How could a CBDC provide privacy to consumers without providing complete anonymity and facilitating illicit financial activity?

If the Federal Reserve moves forward with a digital currency, that currency should use a token-based system that does not rely on distributed ledger technology. The Fed should look to the work of cryptography and digital cash pioneer David Chaum for guidance in implementing a token-based CBDC.

A token-based digital currency issued by the Federal Reserve would present several advantages. First, a token issued by the Federal Reserve could be incorporated into the current banking system, making it easier to adopt a CBDC. Second, it is possible to design a token that replicates the transaction privacy created by physical cash but also implements anti-money laundering protections.[17] This type of CBDC would be a substantial improvement for consumer privacy as payment service providers would not be able to exploit transaction data. Third, by

[17] *See* Chaum 2021 at 12-13.

avoiding a distributed ledger system, a token issued by the Federal Reserve would have affordable transaction costs and be easy to scale up for public use.[18] Fourth, tokens can be designed to expire and need to be refreshed after a certain amount of time, cutting down on currency hoarding and reducing the ability of a central bank to do long term financial surveillance. Expiration dates can ensure that a CBDC is mainly used for transactions.

A token-based CBDC could work with existing intermediaries (banks) and would be able to preserve transaction privacy while allowing for anti-money laundering controls. To accomplish this, currency in the form of tokens would be issued by a central bank, transmitted to users through commercial banks, and encrypted and stored in a digital wallet. To spend the token, the user transmits it to a merchant, who deposits it with the merchant's bank and then the central bank to verify it has not been used before ("double spent"). Using a public/private key pair, merchants can verify the validity of the token using the central bank's public key, but would not receive the payer's private key, maintaining payer anonymity. Similarly, because neither the commercial bank nor the central bank can see the token's unique identifier, a merchant depositing the coin with the central bank does not reveal the individual who withdrew it. Banks would still be able to implement anti-money laundering controls because merchants are identified and verified when their accounts are created. By limiting the amount of currency a merchant can receive in one transaction, and monitoring patterns of payment with merchants, banks and the central bank can conduct strong anti-money laundering activities without compromising privacy for payers.

The Federal Reserve should look to the work to David Chaum to design a CBDC that improves privacy for digital transactions. The following publications are particularly relevant:

- David Chaum, Christian Grothoff, Thomas Moser, *How to issue a central bank digital currency*, Schweizerische Nat. Bank (Mar. 2021),

[18] *Id* at 3.

https://www.snb.ch/n/mmr/reference/working_paper_2021_03/source/working_paper_2021_03.n.pdf.

- David Chaum, Amos Fiat, and Moni Naor, *Untraceable Electronic Cash (extended abstract)*, Advances in Cryptology CRYPTO '88, S. Goldwasser (Ed.), Springer-Verlag, pp. 319-327, https://chaum.com/wp-content/uploads/2021/12/Untraceable_Electronic_Cash.pdf.
- David Chaum, *Privacy Protected Payments Unconditional Payer and/or Payee Untraceability*, SMART CARD 2000, https://chaum.com/wp-content/uploads/2022/02/Privacy-protected-payments-unconditioanal....pdf.

In addition, the Federal Reserve should investigate fully anonymous digital currency and present fully anonymous currency as an option in future publications. The discussion paper discounts the possibility of implementing fully anonymous digital cash due to current anti-money laundering and anti-terrorism laws.[19] However, developing a digital currency will be a long-term process that presents the opportunity to re-think the costs and benefits of those laws. Fully anonymous digital cash may present even greater benefits to privacy, consumer protection, and inclusion for currently unbanked individuals that should be explored. And the use of intermediaries to facilitate the use of CBDCs should make it possible to integrate an anonymous digital payment mechanism through the intermediary while complying with anti-money laundering and fraud regulations as the current system already does with cash deposits and withdrawals. The Fed should investigate and provide an option for fully anonymous digital cash to inform the discussion around CBDC design, and allow the public to weigh in on whether a fully anonymous digital currency is desirable.

Conclusion

EPIC urges the Federal Reserve to foreground privacy and consumer protection as key considerations in their review of digital currency proposals. Because a digital currency by itself will not solve equity, privacy, and fraud harms, the Fed should move slowly to ensure that it does not adopt or encourage use of systems that pose new and significant risks. As part of that review, the Fed

[19] *Money and Payments in the Age of Digital Transformation* supra note 1, at 14.

should undertake a closer review of current data collection and use practices within the digital payment ecosystem and consider the need for greater privacy protections. The Fed should consider a fully anonymous digital cash option for the CBDC, and at a minimum should look towards a token-based CBDC that improves privacy in digital transactions from the status quo. For further questions, please contact EPIC Executive Director Alan Butler at butler@epic.org.

Respectfully Submitted,

Alan Butler
Alan Butler
EPIC Executive Director

Jake Wiener
Jake Wiener
EPIC Law Fellow