We Know What's in Your Wallet: Data Privacy Risks of a Central Bank Digital Currency

Thompson J. Hangen*

TABLE OF CONTENTS

* J.D., May 2023, The George Washington University Law School; Senior Notes Editor, *Federal Communications Law Journal*, Volume 75; B.A., May 2017, Russian and Post-Soviet Studies, The College of William & Mary. I would like to thank Meredith Rose and Natasha Nerenberg for their encouragement, feedback, and support throughout the writing process. I would also like to thank Steve Young for getting me started on learning about blockchain and Matt Gertler for providing opportunities to further develop knowledge in legal issues with blockchain and cryptocurrencies. Finally, I would like to thank my wife for her constant support throughout my law school journey.

I. INTRODUCTION

Governments worldwide are interested in developing and issuing digital currencies, also known as central bank digital currencies ("CBDC," or plural, "CBDCs").[1] A CBDC is issued by a central bank using technology similar to cryptocurrencies[2] and is legal tender.[3] Issuing a CBDC may give governments additional powerful monetary policy tools,[4] but because of the technology involved, also allows governmental agencies to collect massive amounts of identifiable financial data.[5] Where consumer data is collected, consumer data should be protected; when that collection includes every single system transaction, data must be all the more strictly guarded.[6]

The Federal Reserve System ("FRS"), which operates as the central bank in the United States, is responsible for "conducting the nation's monetary policy" and "promoting consumer protection."[7] Implementation of a central bank digital currency in the United States would provide additional policy levers to conduct monetary policy but would also extend the role of the FRS from "promotion" of consumer protection to active collection of consumer data at an unprecedented level.[8] This consumer data would connect an individual to every single financial transaction they, or others connected to

---

1. *See Central Bank Digital Currency Tracker*, ATLANTIC COUNCIL, https://www.atlanticcouncil.org/cbdctracker/ [https://perma.cc/V5XW-2AA7] (last visited Nov. 17, 2021) (tracking development of CBDCs across 90 countries); Turner Wright, *IMF Director: 110 Countries Are 'At Some Stage' of CBDC Development*, COINTELEGRAPH (Oct. 5, 2021), https://cointelegraph.com/news/imf-managing-director-110-countries-are-at-some-stage-of-cbdc-development [https://perma.cc/7YPJ-E7V2].

2. *CBDC vs Cryptocurrency: What Are the Core Differences?*, SHRIMPY ACAD. (May 20, 2021), https://academy.shrimpy.io/post/cbdc-vs-cryptocurrency-what-are-the-core-differences [https://perma.cc/8SCT-6FY6] [hereinafter *CBDC vs Cryptocurrency*].

3. *See* Matthew Green & Peter Van Valkenburgh, *Without Privacy, Do We Really Want a Digital Dollar?*, COIN CTR. (Apr. 30, 2020), https://www.coincenter.org/without-privacy-do-we-really-want-a-digital-dollar/ [https://perma.cc/PAP6-LQN2]. *Contra* Anatoly Kurmanaev et al., *Bitcoin Preaches Financial Liberty. A Strongman Is Testing That Promise*, N.Y. TIMES (Oct. 12, 2021), https://www.nytimes.com/2021/10/07/world/americas/bitcoin-el-salvador-bukele.html [https://perma.cc/83FW-X9DS] (describing how El Salvador has made Bitcoin—a cryptocurrency—legal tender).

4. *See* Brandon Van Niekerk, *Central Bank Digital Currencies: A Technocratic Fallacy*, BITCOIN MAG. (Oct. 17, 2021), https://bitcoinmagazine.com/culture/central-bank-digital-currencies-bitcoin [https://perma.cc/YF4B-FW3E].

5. *See, e.g.*, Ajay S. Mookerjee, *What if Central Banks Issued Digital Currency?*, HARV. BUS. REV. (Oct. 15, 2021), https://hbr.org/2021/10/what-if-central-banks-issued-digital-currency [https://perma.cc/3XU6-8Z26] (discussing how China had collected information on over 500 million transactions by the end of September 2021—mere months after rolling out a limited pilot of a digital Yuan CBDC).

6. *See* Grp. of Seven [G7], *Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs)*, at 7–8 (Oct. 14, 2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1025235/G7_Public_Policy_Principles_for_Retail_CBDC_FINAL.pdf [https://perma.cc/D4AS-5J55] [hereinafter *Public Policy Principles*].

7. *About the Fed*, BD. GOVERNORS FED. RSRV. SYS., https://www.federalreserve.gov/aboutthefed.htm [https://perma.cc/F9Y2-7RRR] (last visited Nov. 22, 2021).

8. *See, e.g.*, *CBDC vs Cryptocurrency*, *supra* note 2.

them, make using a CBDC.[9] While this data could likely be anonymized, it could still be possible to connect an individual to data—including their demographic data, geographic location, financial transaction history, and even the types of personally identifiable information generally collected by banks today to open an account.[10] This massive amount of information carries unique risks for consumers if compromised.[11] Safe implementation of a CBDC requires both stringent legislation aimed at safeguarding consumer data and the institutional competence within the FRS necessary to realize such safeguards.

The Federal Reserve has indicated that development of a CBDC for the United States is a "priority."[12] While development and implementation could take years, appropriate data privacy protections must be built into the development of a CBDC from the outset.[13] Information from the FRS about how a CBDC might be implemented in the United States is still under discussion and may yet include some protection for consumer data.[14] However, adequate data privacy standards, discussed in Section IV below, will likely require an expansion of federal laws (such as the Gramm-Leach-Bliley Act) to cover the unique types of data collected as part of the routine functionality of a CBDC.[15] Such coverage would require Congress to explicitly expand the scope of the FRS.[16]

Interest in a central bank digital currency is not limited to the United States; as of May 2022, at least 87 countries, representing more than 90% of global GDP, are exploring, actively developing, or in the process of implementing a CBDC.[17] Seven countries have fully implemented a CBDC,

9. *See* Van Niekerk, *supra* note 4.

10. *See id.*

11. *See id.* (describing the risk to consumers from the collection of CBDC data as "a perfect honeypot for hackers, fraudsters and the corrupt").

12. Sarah Hansen, *Fed Chair Powell Says Digital Dollar Is a 'High Priority Project'*, FORBES (Feb. 23, 2021, 1:21 PM), https://www.forbes.com/sites/sarahhansen/2021/02/23/fed-chair-powell-says-digital-dollar-is-a-high-priority-project/ [https://perma.cc/6T2E-63BM].

13. *See* BD. OF GOVERNORS OF THE FED. RSRV. SYS, MONEY AND PAYMENTS: THE U.S. DOLLAR IN THE AGE OF DIGITAL TRANSFORMATION 13 (2022) [hereinafter MONEY AND PAYMENTS], https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf [https://perma.cc/QUQ6-LLNB].

14. *See* Andrew Ackerman, *Fed Prepares to Launch Review of Possible Central Bank Digital Currency*, WALL ST. J. (Oct. 5, 2021, 5:30 AM), https://www.wsj.com/articles/fed-prepares-to-launch-review-of-possible-central-bank-digital-currency-11633339800 [https://perma.cc/C3L2-W5WU] (detailing how the Federal Reserve plans to publish a discussion paper on development and use of a CBDC in 2021); MONEY AND PAYMENTS, *supra* note 13, at 19–20 (minimally discussing data privacy concerns in issuance of a CBDC).

15. *See* Fara Soubouti, Note, *Data Privacy and the Financial Services Industry: A Federal Approach to Consumer Protection*, 24 N.C. BANKING INST. 527, 528 (2020) (discussing the need for an expansion of the Gramm-Leach-Bliley Act to include data that commercial banks *already* routinely collect).

16. *See* Christopher J. Waller, Member, Bd. of Governors of the Fed. Rsrv. Sys., CBDC - A Solution in Search of a Problem?, Speech at the American Enterprise Institute 2–3 (Aug. 5, 2021), https://www.bis.org/review/r210806a.pdf [https://perma.cc/T5Y2-CU3B].

17. *See Central Bank Digital Currency Tracker*, *supra* note 1; Wright, *supra* note 1.

and an additional seventeen are currently piloting one.[18] At the 2021 G7 Summit, member countries[19] released thirteen principles to which a CBDC should adhere, demonstrating the importance of near-term CBDC development to major world economies.[20] The G7 recognized that each nation's data privacy laws differ but agreed that generally, a CBDC "must protect the privacy of users, including by requiring that the processing of their personal data is subject to laws governing privacy and the collection, storage, safeguarding, disposal and use of personal data that are enforceable in the jurisdiction."[21] However, notwithstanding the emergence of CBDCs worldwide, there exists no comprehensive data privacy standards or guidelines that countries can use as a benchmark for consumer data protection.[22]

To address these interests, Congress should explicitly expand the scope of the FRS.[23] Section II.A of this Note provides a high-level discussion of technologies used to create blockchains and how they can be used to create a centralized ledger for central bank digital currencies, as well as a discussion of how CBDCs differ from more common cryptocurrencies. Section II.B considers the case for and against issuance of a CBDC, including data privacy concerns. Section III reviews how federal financial data privacy laws (especially the Gramm-Leach-Bliley Act) currently provide for consumer data protection and storage, and the extent to which such laws might cover CBDC-related data.[24] Section IV urges Congress to enact a unified data privacy standard that encompasses CBDC data and to empower the Federal Reserve System to collect, safely store, and protect consumer data. Section V

18. *See Central Bank Digital Currency Tracker*, *supra* note 1; Jinia Shawdagor, *Asian CBDC Projects: What Are They Doing Now?*, COINTELEGRAPH (Oct. 16, 2021), https://cointelegraph.com/news/asian-cbdc-projects-what-are-they-doing-now [https://perma.cc/E276-K62S]; *Bank of England Mulls CBDC Models in Technology Engagement Forum*, LEDGER INSIGHTS (Oct. 21, 2021), https://www.ledgerinsights.com/bank-of-england-mulls-cbdc-models-in-technology-engagement-forum/ [https://perma.cc/TY94-DMEF]; Tom Farren, *Hong Kong Exploring CBDC as Part of Fintech Strategy*, COINTELEGRAPH (Oct. 4, 2021), https://cointelegraph.com/news/hong-kong-exploring-cbdc-as-part-of-fintech-strategy [https://perma.cc/8XGH-ZP3H].

19. *See G7 UK 2021*, GOV.UK, https://www.g7uk.org/ [https://perma.cc/9XWQ-3N75] (last visited Nov. 22, 2021) (including, in this instance Australia, India, South Korea, and South Africa).

20. *See Public Policy Principles*, *supra* note 6, at 4–5.

21. *Id.* at 7–8.

22. *Id.* (recognizing that CBDC "ecosystems" should "consider" how to ensure data privacy of consumers, and "be aligned to the progress being made towards international standards," while declining to create such standards).

23. *See* Waller, *supra* note 16, at 2–3.

24. While data privacy provisions exist in state laws, *see, e.g.*, California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (West 2018), and international data privacy standards, *e.g.*, CROSS BORDER PRIVACY RULES SYSTEM, http://cbprs.org/ [https://perma.cc/UPM6-VLGX] (last visited Nov. 22, 2021), a review of state law and international standards is beyond the scope of this Note. Additionally, a full survey of federal data privacy law is beyond the scope of a Note of this length.

concludes by proposing a mechanism to implement data privacy standards for CBDC use.

II. BACKGROUND

This section covers the basics of how blockchain technology works, and how a central bank digital currency might be implemented. It also discusses how a CBDC compares to other forms of digital currency and what benefits and risks they might contain.[25]

A. While a Central Bank Digital Currency May Be Built on a Blockchain, it is Distinct from Cryptocurrencies or Other Digital Ledger Tokens

While blockchain-based technologies are increasingly in the public eye, they remain an emerging area of technology and law. Accordingly, a non-technical primer of blockchain technologies, how the technology operates, what use cases exist, and what a CBDC is follows.

1. Blockchain Technologies Combine Existing Technologies into a Ledger-Based Tool for Storing and Distributing Information

Blockchain is not a new technology; rather, it is a novel combination of existing technologies to allow for the decentralized storage and distribution of information.[26] Blockchain combines concepts such as peer-to-peer networks (e.g., the Internet), cryptographic keys (used in many secure messaging systems), democratic consensus mechanisms, and digital signatures.[27] The resulting combination allows for a unique system of storing and distributing information: a decentralized ledger that shows up-to-date information on ownership of assets and how entities have interacted with each other over time (i.e., a ledger of transactions between blockchain participants).[28]

25. A full, technical discussion of how blockchains operate and all forms of digital currency is beyond the scope of a Note of this length. The following material provides a brief primer on essential principles.

26. CHRIS JAIKARAN, CONG. RSCH. SERV., R45116, BLOCKCHAIN: BACKGROUND AND POLICY ISSUES 1–2 (2018).

27. *Id.*; *see also* PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 2–3 (2018).

28. *See* DE FILIPPI & WRIGHT, *supra* note 27, at 3 ("[B]lockchain technology supports decentralized, global value transfer systems that are both transnational and pseudonymous . . . . Governments across the globe are experimenting with blockchains to secure and manage critical public records, including vital information and titles or deeds to property.").

The Internet itself exists as a series of protocols that define how individuals can interact with it.[29] These protocols are a universal language that any computer or device must "speak" to access the Internet, and as such, they draw limits around what can or cannot be done by people interacting with the network.[30] Traditionally, governments have been able to implement layers of protocol that prohibit or enable certain actions, allowing for control over digital content and actions of citizens within their borders.[31] Blockchain technologies exist as another layer of protocol, analogous to another "application" layer.[32] Blockchain protocols allow individuals to interact with the defined protocol to access information on ownership and submit changes (generally being transactions between users) to that information.[33] Whether those changes are accepted relies on how the protocol of the blockchain is defined.[34]

Blockchains typically use peer-to-peer networks: a distributed network where participating computers connect with each other in a one-to-many relationship, rather than each computer connecting to a central server.[35] Each computer in the network communicates using the same blockchain protocol to validate, store, and distribute information.[36] By storing the complete transactional history of the blockchain on each participant computer, the network is resistant to change, and information is validated by consensus.[37] If a majority of participant computers validate a transaction stored in the ledger, that "block" of transactions is added to the "chain"—forming a comprehensive ledger of all previous transactions.[38] Accordingly, blockchains are largely autonomous, where changes to the blockchain are implemented through democratic consensus mechanisms rather than a central authority.[39]

---

29. *See* ALEXANDER R. GALLOWAY, PROTOCOL: HOW CONTROL EXISTS AFTER DECENTRALIZATION 38–39 (2004).

30. *See id.* at 46–47.

31. *See* DE FILIPPI & WRIGHT, *supra* note 27, at 50–51. *But cf.* Eric Hughes, *A Cypherpunk's Manifesto*, ACTIVISM.NET (Mar. 9, 1993), https://www.activism.net/cypherpunk/manifesto.html [https://perma.cc/3PD6-GWT4] (defining core values of the cypherpunk movement (a precursor movement to the development of cryptocurrencies), including advocating for privacy, freedom of information, the right to anonymity, and a lack of government monitoring and censorship).

32. *See* GALLOWAY, *supra* note 29, at 130.

33. *See* DE FILIPPI & WRIGHT, *supra* note 27, at 54–55.

34. *Id.*

35. *See id.* at 42–45.

36. *See id.*

37. *See id.* at 42 ("Underlying each blockchain-based network is a consensus mechanism that governs how information can be added to the shared repository. Consensus mechanisms make it possible for a distributed network of peers to record information to a blockchain, in an orderly manner, without the need to rely on any centralized operator . . . .").

38. *See id.* at 42–45.

39. *See* DE FILIPPI & WRIGHT, *supra* note 27, at 42–45, 147–48. A blockchain-based network and system can even lead to the creation of a decentralized autonomous organization (DAO), which is "a particular kind of decentralized organization that is neither run nor controlled by any person but entirely by code" and "generally consist[s] of a collection of smart contracts that do not have any 'owner.'" *Id.*

Blockchain users maintain a private key[40] (a lengthy alphanumeric code) known only to them.[41] As demonstrated in Figure 1, below, this private key is used as the input for a cryptographic algorithm to generate a public key, which is used to publicly sign transactions.[42] A public key is unique to a single private key, and users maintain it by keeping the private key confidential.[43] While a user may input a private key to access the blockchain, only the output of the cryptographic algorithm (the public key) is stored within the blockchain ledger.[44] Knowledge of the public key does not necessarily reveal any information about the user, although it may mean that an individual's transactions may be tracked if the public key is connected to the user.[45]

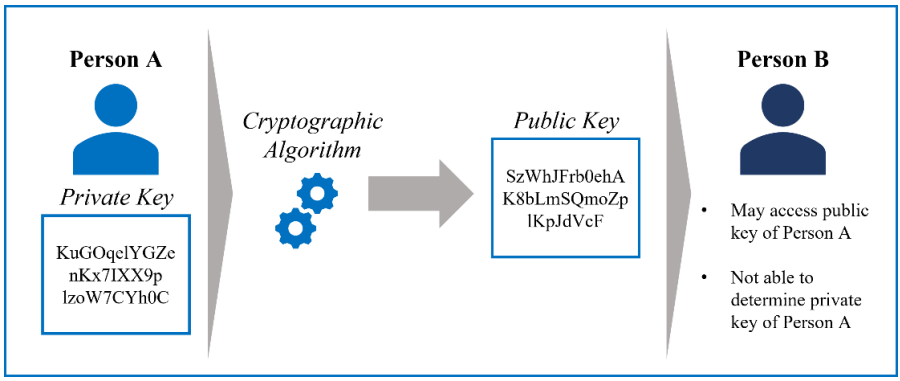

Figure 1: Private Keys Sign Transactions, Revealing a "Public Key" and Protecting User Anonymity

40. *See id.* at 38–39.

41. A private key is used in lieu of the more familiar process of signing into a secure website, wherein one enters a username and password, which is validated against a secure, central server. *See* Philip Bates, *How Do Websites Keep Your Passwords Secure?*, MUO (July 7, 2021), https://www.makeuseof.com/tag/websites-keep-passwords-secure/ [https://perma.cc/7P2S-UH5T]. The pitfalls of such a system are familiar: a compromised email address could be used to reset passwords associated with that email address, giving hackers access to multiple logins. *See id.* Alternatively, the central server could be hacked, compromising the username and password combinations of many users at once, unless otherwise encrypted. *See id.*

42. *See* JAIKARAN, *supra* note 26, at 1–2.

43. *Id.*

44. *Id.*

45. *Id.*

2. A Central Bank Digital Currency is Distinct from Cryptocurrencies and Stablecoins

While blockchains have many potential use cases,[46] one of the most common is in creating digital currencies, known as cryptocurrencies.[47] The fundamental information stored on a blockchain are digital assets or tokens, which have "money-like characteristics" and are used as a means of exchange for goods and services.[48] A user interacts with the blockchain by creating an account (often called a wallet) that has a private and public key.[49] The public key is used to create an address to which other users can send cryptocurrency tokens in some amount.[50] The blockchain stores the transactional data and proof of ownership in a series of coded "blocks," which maintains the informational integrity of the system: an anonymized, complete financial history of the transactions and interactions with the cryptocurrency blockchain.[51] Users participate in the blockchain by using their wallets to process transactions or by participating in "mining" of new blocks in the chain.[52] Mining blocks adds to the blockchain, allowing the transactional history of the network to continue to grow.[53] Mining rewards (e.g., tokens awarded for successfully "mining" a block) incentivize users to utilize the processing power of their computers[54] to help manage the decentralized blockchain.[55] Notably, in most blockchains, new tokens are only generated through mining and are not issued by a centralized body; anyone may participate, and anyone who participates may be rewarded for their successful participation.[56] A user typically acquires additional cryptocurrency by mining, by purchase on cryptocurrency exchanges, or by exchange (e.g., sale

46. *See, e.g.*, Jamie Berryhill et al., *Blockchains Unchained: Blockchain Technology and Its Use in the Public Sector* 13–15 (Org. for Econ. Coop. & Dev., Working Paper No. 28, 2018) (providing specific case studies for how blockchain technologies have been used in public sector applications (e.g., creation of a land registry to track ownership of land assets, inter-bank payments of international monetary or government securities transactions, or asset tracking for car ownership)).

47. *See* JAIKARAN, *supra* note 26, at 3, 5–6.

48. *See id.*

49. *See id.*

50. *See id.*; *see also CBDC vs Cryptocurrency*, *supra* note 2.

51. *See* DE FILIPPI & WRIGHT, *supra* note 27, at 42–45 (describing the term "blockchain"—a series of blocks "chained" together in series, creating an unchangeable, immutable ledger of past transactions using the blockchain-based system).

52. *See* Euny Hong, *How Does Bitcoin Mining Work?*, INVESTOPEDIA, https://www.investopedia.com/tech/how-does-bitcoin-mining-work/ [https://perma.cc/K52P-3NFX] (last visited Jan. 29, 2022).

53. *See id.*

54. Mining often utilizes specialized, networked equipment to "mine" on cryptocurrency networks. *See* Hong, *supra* note 52. A full discussion of the various hardware used for cryptocurrency blockchain engagement is not within the scope of this Note.

55. *See id.*

56. *See id.*

of goods or services in exchange for cryptocurrency).[57] The value of a cryptocurrency is dependent on the cost of production, the extent to which the community is involved in the blockchain, and general demand.[58] Accordingly, cryptocurrencies have been faulted for their extreme volatility.[59] Cryptocurrency blockchains also evolve over time as participants in the network participate in decentralized, democratic processes to vote on changes in the code.[60] If consensus is reached, the blockchain adopts the code-based amendment.[61]

Less common are stablecoins: cryptocurrencies with a value that is equivalent or "pegged" to a fiat currency (e.g., the U.S. dollar).[62] Stablecoins typically have a decentralized, peer-to-peer ledger and network, similar to cryptocurrencies.[63] The mechanism for creating additional stablecoins differs from cryptocurrencies: instead of creating new tokens by a user participation mining process, stablecoins are backed by fiat currency.[64] As users purchase stablecoins, the funds used to purchase the stablecoin are held as collateral to back the stablecoin, providing liquidity.[65] Often, cryptocurrency exchanges will use stablecoins as the necessary on- and off-ramps for users to exchange between cryptocurrencies and fiat currency; users exchange fiat currency for an equivalent amount of a stablecoin (e.g., U.S. dollar for the "USD coin" or USDC), and from there to cryptocurrency.[66] When users want to convert their cryptocurrency back to fiat currency, they are often forced to convert from cryptocurrency to stablecoin and finally back into fiat currency.[67] Apart from

57. *See id.*; *see also CBDC vs Cryptocurrency*, *supra* note 2. Additionally, participants in a blockchain-based system may acquire cryptocurrencies through a process known as "staking," wherein users lock up a certain amount of cryptocurrency in "validator" pools that earn interest over time. *See* Krisztian Sandor, *Crypto Staking 101: What Is Staking?*, COINDESK (Apr. 1, 2022, 11:37 AM), https://www.coindesk.com/learn/crypto-staking-101-what-is-staking/ [https://perma.cc/2HTA-264D].

58. *See* Hong, *supra* note 52; *see also CBDC vs Cryptocurrency*, *supra* note 2.

59. *See* Nicole Lapin, *Explaining Crypto's Volatility*, FORBES (Dec. 23, 2022, 6:00 AM), https://www.forbes.com/sites/nicolelapin/2021/12/23/explaining-cryptos-volatility [https://perma.cc/TJ9R-B87A].

60. *See What Are Blockchain Forks?*, CMC MARKETS, https://www.cmcmarkets.com/en/learn-cryptocurrencies/what-is-a-blockchain-fork [https://perma.cc/7ZKY-C5H8] (last accessed Sept. 29, 2022).

61. *See id.*

62. Fiat currency is a government-issued currency, specifically one not backed by a commodity (e.g., precious metals). *See* James Chen, *Fiat Money*, INVESTOPEDIA, https://www.investopedia.com/terms/f/fiatmoney.asp [https://perma.cc/VB4V-PZ8B] (last visited Mar. 5, 2022). Instead, the value backing the currency is the strength and stability of the government issuing the currency. *See id.*

63. *See* Adam Hayes, *Stablecoin*, INVESTOPEDIA, https://www.investopedia.com/terms/s/stablecoin.asp [https://perma.cc/A4R7-43YC] (last visited Apr. 9, 2022).

64. *See id.*

65. *See id.* (indicating that stablecoins may actually be either fiat-collateralized or crypto-collateralized, but in either form, some store of value is used as collateral and to provide liquidity as needed).

66. *See id.*

67. *See, e.g.*, *Withdrawals*, COINBASE, https://help.coinbase.com/en/commerce/getting-started/withdrawals [https://perma.cc/SLH3-W2XD] (last visited Sept. 29, 2022).

the mechanism of backing stablecoins with fiat currency, they are essentially indistinguishable from a cryptocurrency.[68]

A central bank digital currency (CBDC) differs from a cryptocurrency in four main ways: (1) the network model, (2) how the price of the token is determined, (3) the extent to which user information is stored on the blockchain, and (4) how changes to the blockchain are managed.[69] First, the network model in a CBDC is typically centrally managed, as opposed to a peer-to-peer, decentralized network.[70] The entire CBDC blockchain would be functionally under the control of the Federal Reserve, even if the development were outsourced to a third party.[71] The Federal Reserve would necessarily maintain an application programming interface (API) allowing CBDCs to be issued to commercial banks or directly to users.[72] Second, the price of the token is determined in the same way as fiat currency: through carefully managed monetary policy from the issuing authority.[73] In other words, a CBDC would be issued as "a digital liability of the Federal Reserve that is widely available to the general public."[74] A CBDC could be directly issued to other banks or private parties without mechanisms such as deposit insurance or backing by an underlying asset pool.[75] Third, use of a CBDC would necessarily require users to reveal personal information (e.g., the same information traditionally used to open a bank account: name, SSN, verification of identification, etc.).[76] A CBDC would also generate data about users' financial transactions and history, not unlike the financial data that is generated today.[77] However, this data would include the entire web of transactional data between users: showing how each CBDC came to be in each individual's wallet.[78] Such transaction history would theoretically be centralized with the blockchain manager (the Federal Reserve), even if minimally anonymized by using a public-private key encryption model

68. *See, e.g.*, Hayes, *supra* note 63 ("A stablecoin is a class of cryptocurrencies that attempt to offer price stability and are backed by a reserve asset. Stablecoins . . . offer the best of both worlds—the instant processing and security or privacy of payments of cryptocurrencies, and the volatility-free stable valuations of fiat currencies.").

69. *See CBDC vs Cryptocurrency*, *supra* note 2.

70. *See* Van Niekerk, *supra* note 4. Note that the introduction of various bills in Congress, including the Electronic Currency And Secure Hardware Act (ECASH Act) may—if passed into law—both (a) authorize the FRS to issue a CBDC and (b) prohibit the use of "a decentralized ledger (or indeed, any ledger of any type), which its proponents argue will help preserve user privacy." Nikhilesh De, *Lawmakers Keep Mentioning Privacy in CBDC Discussions*, COINDESK (Apr. 5, 2022, 5:16 PM), https://www.coindesk.com/policy/2022/04/05/lawmakers-keep-mentioning-privacy-in-cbdc-discussions/ [https://perma.cc/PW6S-LSR4]. It is unclear how a CBDC might be issued without any ledger system showing asset ownership. *Id.*

71. *See* Van Niekerk, *supra* note 4.

72. *See id.*

73. *See CBDC vs Cryptocurrency*, *supra* note 2.

74. MONEY AND PAYMENTS, *supra* note 13, at 13.

75. *See id.*

76. *See id.* at 13, 19.

77. *Id.* at 19.

78. *See* De, *supra* note 70.

similar to cryptocurrency.[79] Fourth, changes to the underlying protocol of a CBDC network would be determined and implemented by the issuing authority—the central bank—as opposed to a consensus-based user participation model.[80] Changes to the protocol would have a material (and potentially adverse)[81] impact on the user, as addressed below.[82]

B. A Central Bank Digital Currency Gives Powerful Monetary Policy Tools to the Government but Poses Inherent Privacy Risks

A central bank digital currency could substantially modernize our financial system.[83] Doing so could benefit consumers in the U.S. and maintain the strength of the U.S. dollar worldwide.[84] However, doing so without implementing effective safeguards could compromise consumer data.[85] Whether or not the benefits of a CBDC outweigh the risks remains to be seen; however, CBDC development is unlikely to begin until risks are adequately addressed.[86]

1. A Central Bank Digital Currency Provides Monetary Policy Tools to Ensure Equitable Access to Online Financial Payment Methods

The Board of Governors for the Federal Reserve System released a report in January 2022 detailing five benefits of a central bank digital currency.[87] First, a CBDC would "safely meet future needs and demands for payment services."[88] For example, as the economy increasingly goes "digital," a CBDC could be used as digital cash for online transactions.[89] A CBDC could lessen credit and liquidity risks to individual users by providing easy access to a digital "cash" form of money.[90] Instead of using credit or debit cards and accounts, consumers could directly pay for online transactions using a CBDC as digital cash (whereas the current system requires days or

79. *See* Van Niekerk, *supra* note 4.
80. *See id.*; *CBDC vs Cryptocurrency*, *supra* note 2.
81. *See, e.g.*, Tim Hakki, *Edward Snowden: CBDCs Are 'Cryptofascist Currencies' That Could 'Casually Annihilate' Savings*, DECRYPT (Oct. 10, 2021), https://decrypt.co/83124/edward-snowden-cbdcs-are-cryptofascist-currencies-that-could-casually-annihilate-savings [https://perma.cc/8XCG-WFU7] (highlighting concerns that "negative interest rates" could be used to encourage spending, which could be used as a tool to spur economic growth).
82. *See, e.g.*, MONEY AND PAYMENTS, *supra* note 13, at 17.
83. *See id.* at 13.
84. *See id.* at 15.
85. *See* Van Niekerk, *supra* note 4.
86. *See* MONEY AND PAYMENTS, *supra* note 13, at 19–20.
87. *See id.* at 14–16.
88. *Id.* at 14.
89. *Id.* at 15.
90. *See id.* at 14–15.

weeks to reconcile transactions).[91] Second, a CBDC could lead to "improvements to cross-border payments."[92] In fact, limited trials have shown that cross-border payments can be made using CBDCs in seconds, instead of the current "three to five days."[93] Not only would the time savings represent significant efficiency gains over the current system for cross-border payments, but using a CBDC would reduce the costs of such payments by up to 50%.[94] Third, a CBDC would "support the dollar's international role."[95] Recognizing that the dollar is widely used internationally, easy access to a CBDC could help ensure widespread use and adoption of the U.S. dollar (e.g., preventing decrease in dollar usage as other countries adopt easily accessible CBDC using their own currencies or CBDCs released by other nations).[96] Fourth, a CBDC could reduce barriers and lower transactional costs to "financial inclusion,"[97] benefitting low-income and unbanked households.[98] Fifth, a CBDC would "extend public access to safe central bank money," especially in an increasingly digital world.[99] Use of a CBDC would provide the online equivalent to using cash online, rather than relying on traditional payment systems which carry credit and liquidity risks.[100]

Use of a CBDC places monetary tools into the hands of the Federal Reserve System to accomplish the benefits described above.[101] Choices in the design and implementation of a CBDC would affect how users perceive and use a CBDC system.[102] For example, the amount of interest a CBDC would accrue could be changed at will to encourage spending or saving as a tool against inflation.[103] Protocols could also facilitate the rapid payment of taxes, tax refunds, delivery of wages, and access to credit.[104] Possibly some of these additional features could drive adoption of a CBDC; some users who might

91. *See id.*

92. MONEY AND PAYMENTS, *supra* note 13, at 15.

93. Alun John, *Central Bank Digital Currencies Can Slash Cross Border Payment Time*, REUTERS (Sept. 28, 2021, 3:07 AM), https://www.reuters.com/business/central-bank-digital-currencies-can-slash-cross-border-payment-time-bis-2021-09-28/ [https://perma.cc/7NPY-LHDT].

94. *See id.*

95. MONEY AND PAYMENTS, *supra* note 13, at 15.

96. *See id.*

97. *Id.* at 16.

98. *Id.* (stating that further study is necessary to assess the potential for CBDC to help "underserved and lower income households"). *Contra* Waller, *supra* note 16, at 2–3 (suggesting that less than 1% of American households are both unbanked *and* potentially interested in a CBDC account issued by the Federal Reserve System).

99. MONEY AND PAYMENTS, *supra* note 13, at 16.

100. *See id.* (describing how cash use in the United States has decreased from 40% of transactions in 2012 to 19% of transactions in 2020, a trend that is likely to continue).

101. *See id.* at 16–17.

102. *See id.* at 17.

103. *See, e.g.*, *id.* (suggesting that a "non-interest-bearing CBDC" could make CBDC use "less attractive as a substitute for commercial bank money" and therefore limit changes to the traditional financial-sector); *see also* Hakki, *supra* note 81.

104. *See* MONEY AND PAYMENTS, *supra* note 13, at 16.

not see the utility in "digital cash" may nevertheless use a CBDC if it provides an easier way to handle taxes or access credit.[105]

2. Data Aggregation Creates Significant Risk for Consumer Data Privacy

The Federal Reserve System paper on CBDCs flags "complex policy issues and risks" that could benefit from additional scholarship and analysis.[106] CBDC usage could lead to widespread "changes to financial-sector market structure[s]."[107] Banks traditionally rely on central bank deposits to fund loans to consumers; a CBDC would provide direct competition with commercial bank money and could result in "increased bank funding expenses . . . and reduce credit availability or raise credit costs for households and businesses" as the aggregate value of central bank deposits in commercial banks decreases.[108] Direct consumer access to a CBDC could make "runs on financial firms more likely or severe," undercutting safeguards currently in place to prevent bank runs.[109] Over time, to the extent that CBDCs provide simplified access to credit options, use of commercial banks could decline precipitously, especially given the increasing digitization of commerce.[110]

An important area of risk for the Federal Reserve is ensuring "privacy and data protection and the prevention of financial crimes."[111] There is a balancing act between the necessity of preventing financial crimes and the necessity of data privacy and protection.[112] Perfect financial information would all but negate the possibility for financial crimes, whereas complete anonymity would afford protection of consumer data but provides ample

105. *See* Waller, *supra* note 16, at 2–3.

106. MONEY AND PAYMENTS, *supra* note 13, at 17. A full discussion of all of the complex policy issues and risks contained in the FRS paper is beyond the scope of this Note: indeed, additional scholarship is needed to continue to address the potential risks of a CBDC system.

107. *Id.*

108. *Id.* (suggesting also that the increase in cryptocurrency and stablecoin use poses similar risks to commercial banks). *Contra* Hughes, *supra* note 31 (defining the radical transformation of traditional systems, which forms the core of the cypherpunk movement—leading to the initial development of cryptocurrencies: such a transformation to the financial-sector market structure is in-line with the earliest goals of the cryptocurrency movement).

109. MONEY AND PAYMENTS, *supra* note 13, at 17.

110. *See, e.g.*, *id.*

111. *Id.* at 19.

112. *See* MONEY AND PAYMENTS, *supra* note 13, at 19.

ground for the growth and proliferation of underworld financial schemes.[113] Some level of collection of consumer data is essential with a CBDC to support anti-money laundering (AML) policy goals and would likely involve similar data to what is now collected from consumers in opening a bank account.[114]

The Federal Reserve System waves aside such concerns, stating that an intermediary system would be used to issue CBDCs, and those intermediaries (i.e., commercial banks) would utilize "existing tools" to collect and protect consumer data.[115] This argument ignores a fundamental conflict of interest: CBDC funds operate in direct competition with commercial bank funds, offering limited incentive for commercial banks to offer CBDC accounts to users.[116] For this very reason, many countries are likely to adopt a direct-to-consumer CBDC issuance system.[117] Such a system necessarily requires the "digitization and centralization of identity" to verify user information and limit the possible commission of financial crimes.[118] This places personally identifiable information in the hands of the Federal Reserve System and then connects that information explicitly to the spending habits and practices of individuals.[119]

Even in an intermediated system where personally identifiable information is not maintained by the Federal Reserve, the data privacy risks posed by a CBDC are expansive. The Federal Reserve would have access to an unprecedented aggregation of consumer financial data, including a ledger showing the complete and accurate ownership of all assets by account, as well as a list of every transaction from account to account.[120] This would allow the tracing of a single CBDC dollar from issuance to the current account holder.[121] Imagine that the government knew not only how much money was in your wallet, but the serial numbers of every dollar bill in your wallet and how it came to be there.[122] This is such a radical shift from the current baseline

113. *See id.* Fears that criminals might want to use a CBDC are overstated. *See* Tom Sadon, *5 Reasons Why Criminals & Terrorists Turn to Cryptocurrencies*, COGNYTE (Nov. 2, 2021), https://www.cognyte.com/blog/5-reasons-why-criminals-are-turning-to-cryptocurrencies/ [https://perma.cc/PXY3-ABH3] (stating that criminals may use cryptocurrencies because they offer some privacy, are not centrally managed, can process transactions quickly, and are borderless). While criminals occasionally use cryptocurrencies, their reasons for doing so are, in effect, the list of differences between a cryptocurrency and a CBDC. *See id.* A CBDC has no such promise of anonymity or privacy and is centrally managed by the U.S. government—which tends to support a preliminary hypothesis that a CBDC would not be attractive to the criminal underworld. *See, e.g.*, *id.*

114. *See* MONEY AND PAYMENTS, *supra* note 13, at 17–18.

115. *See id.* at 13–14, 17.

116. *See id.* at 17, 19.

117. *See Central Bank Digital Currency Tracker*, *supra* note 1.

118. Van Niekerk, *supra* note 4.

119. *See, e.g.*, *id.* (detailing the connection from digitization and centralization of identity to use of CBDC systems as a method for digital signatures, access to government services, and linking payments to individual identity).

120. *See id.*

121. *See CBDC vs Cryptocurrency*, *supra* note 2.

122. *See id.*; Van Niekerk, *supra* note 4.

that it is not considered by current data privacy law.[123] Granted, in an intermediary system, such data may be anonymized,[124] but the personal nature of spending habits is a factor in some transactions that remain in cash today.[125] Even when anonymized, use of a CBDC would place the entire web of financial transaction data in the hands of the federal government, and "with great power comes great responsibility"—in this case, the need to create robust federal data privacy protections.[126]

III. FEDERAL FINANCIAL DATA PRIVACY: THE GRAMM LEACH-BLILEY ACT

United States data privacy law is a multijurisdictional patchwork of state and federal laws.[127] The most significant federal law establishing data privacy standards for financial institutions is the Gramm-Leach-Bliley Act ("GLBA").[128] While some state laws may exceed the data privacy standards in the GLBA,[129] these state laws cannot be enforced against the federal government.[130] Some state laws, like the California Consumer Privacy Act, may provide a helpful model for expanding federal data privacy protections to consumers.[131] However, state laws are less relevant to a discussion of the issuance of central bank digital currencies by the Federal Reserve—a federal agency and accordingly, an in-depth discussion of state data privacy law is out of scope for this Note.[132] This section proceeds with an analysis of the GLBA: its history and legislative purpose, relevant data privacy provisions, and the applicability of the GLBA to federal agencies as financial institutions.The Gramm-Leach-Bliley Act was signed into law in 1999 in an effort to "enhance competition in the financial services industry by providing a prudential framework for the affiliation of banks, securities firms, insurance

123. *See* Soubouti, *supra* note 15, at 534–35.

124. *See* MONEY AND PAYMENTS, supra note 13, at 19.

125. *See id.* at 16; Waller, *supra* note 16, at 4.

126. *See* Aaron Gleason, *Steve Ditko's Great Gift to the World: 'With Great Power Comes Great Responsibility'*, FEDERALIST (July 9, 2018), https://thefederalist.com/2018/07/09/steve-ditkos-great-gift-world-great-power-comes-great-responsibility/ [https://perma.cc/KQ8Z-5LXB] (describing the origins of the phrase as likely dating to the allegory of the Sword of Damocles—perhaps another apt metaphor for the data privacy concerns posed by a CBDC); *see also* Van Niekerk, *supra* note 4.

127. *See* Soubouti, *supra* note 15, at 527–28.

128. *See id.* at 528–29.

129. *See id.* at 531.

130. McCulloch v. Maryland, 17 U.S. 316, 426 (1819) ("This great principle is, that the constitution and the laws made in pursuance thereof are supreme; that they control the constitution and laws of the respective states, and cannot be controlled by them.").

131. *See* Meredith E. Bock, Note, *Biometrics and Banking: Assessing the Adequacy of the Gramm-Leach-Bliley Act*, 24 N.C. BANKING INST. 309, 321–22 (2020); California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.140(b) (West 2018).

132. *See* Bock, *supra* note 131, at 321–22.

companies, and other financial service providers"[133] The GLBA applies to "financial institutions," creating an affirmative duty to "respect the privacy of its customers" and to protect customer "nonpublic personal information."[134] "Nonpublic personal information" is defined as "personally identifiable financial information (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution."[135]

Exceptions to "nonpublic personal information" exist for information that is publicly accessible.[136] In other words, a consumer may expect that financial institutions (such as a bank) will safeguard any personal information she explicitly provides (including, e.g., name, date of birth, SSN, address, income information)[137] as well as information related to transactions with the bank.[138] A consumer using a credit card provided by a commercial bank, therefore, should not expect that any transactions using the credit card are private.[139] However, a consumer using cash withdrawn from a bank ATM may expect that any transactions using that cash are private; the bank is only aware of the fact that a certain amount of cash was withdrawn at an ATM by that user, not what happens to the cash after the fact.[140] Financial institutions must provide privacy and opt-out notices to inform customers of data privacy policies and provide a mechanism for individuals to opt-out of a financial institution sharing information with "nonaffiliated third parties."[141] Financial institutions must also maintain customer data safely and securely.[142]

The GLBA has been held to apply to federal institutions such as "credit reporting agencies."[143] Indeed, the text of the GLBA states that it applies to each "agency or authority" that is a "financial institution."[144] A "financial institution" includes any institution engaged in "financial activities," excluding institutions that do not "sell or transfer nonpublic personal

133. Individual Reference Servs. Grp., Inc. v. FTC, 145 F. Supp. 2d 6, 17 (D.D.C. 2001), *aff'd sub nom.* Trans Union LLC v. FTC, 295 F.3d 42 (D.C. Cir. 2002) (quoting H.R. REP. NO. 106-434, at 245 (1999) (Conf. Rep.)).

134. 15 U.S.C. § 6801(a).

135. 15 U.S.C. § 6809(4)(A).

136. 15 U.S.C. § 6809(4)(B).

137. *See* Bock, *supra* note 131, at 315.

138. *See* 15 U.S.C. § 6801(a).

139. *See, e.g.*, Bock, *supra* note 131, at 315.

140. *See, e.g.*, Brad Berens, *Why Using Cash Won't Protect Your Privacy*, CTR. DIGIT. FUTURE (Jan. 4, 2018), https://www.digitalcenter.org/columns/cash-and-anonymity/ [https://perma.cc/R3UH-R7XJ]. Such an analogy breaks down when the cash is replaced with a digital token that is tracked. If either a commercial bank or the Federal Reserve System is aware of every single issued CBDC "dollar"—where it is, how it got there, and who currently owns it—then either institution has access to data that was not considered under the GLBA or other federal data privacy laws. *See* 15 U.S.C. § 6809(4)(A).

141. *See* Bock, *supra* note 131, at 315–16.

142. *See* Bock, *supra* note 131, at 315–16.

143. *Individual Reference*, 145 F. Supp. 2d at 17 (quoting H.R. REP. NO. 106-434, at 245).

144. 15 U.S.C. § 6801.

information to a nonaffiliated third party."[145] The FRS does not currently collect consumer data. In fact, the Federal Reserve Act "does not authorize direct Federal Reserve Accounts for individuals, and such accounts would represent a significant expansion of the Federal Reserve's role in the financial system and the economy."[146] The issue of whether the GLBA applies to the FRS is therefore currently moot.[147] However, if individuals were issued CBDC funds directly from the FRS, the FRS would undoubtedly fall under and be required to follow the requirements of the GLBA.[148]

The GLBA does not require financial institutions to safeguard consumer data that is not protected by the Act.[149] This includes information gathered on websites from visitors or non-customers, including "behavioral biometric data."[150] Behavioral biometric data includes keystrokes and navigation of a webpage to verify a user's identity; such data can create a unique user profile to identify users who do not provide data otherwise covered by the GLBA.[151] This kind of data is currently used in fraud detection by financial institutions to highlight anomalous customer behavior.[152] CBDC data could provide a similar "user profile" constructed of all of a user's transactions using digital cash.[153] Such data would contain an interwoven mixture of protected and unprotected data.[154] To the extent that data is not currently protected by the GLBA, financial institutions may have little incentive to safeguard user data. Accordingly, as discussed below, the scope of the GLBA should be amended to include the data types that would be collected in use of a CBDC.

IV. PROPOSED DATA PRIVACY STANDARDS FOR CENTRAL BANK DIGITAL CURRENCIES

A. The Federal Reserve System Has Not Addressed Data Privacy Concerns Inherent in CBDCs

Use of a CBDC would necessarily involve the widespread collection and use of consumer data.[155] As discussed previously, consumers would not only furnish the types of data used in setting up a bank account to initially set up a wallet for CBDC use, but would also necessarily consent to the collection

145. 15 U.S.C. § 6809(3).
146. MONEY AND PAYMENTS, *supra* note 13, at 19.
147. *See id.* at 13–14.
148. 15 U.S.C. § 6809(3).
149. *See, e.g.*, 15 U.S.C. § 6809(4).
150. *See* Soubouti, *supra* note 15, at 534-35; Bock, *supra* note 131, at 313.
151. *See* Bock, *supra* note 131, at 313.
152. *See id.*
153. *Id.* at 313; *see also* Van Niekerk, *supra* note 4; *CBDC vs Cryptocurrency*, supra note 2.
154. *See, e.g.*, Van Niekerk, *supra* note 4.
155. *See id.*

of all transaction data.[156] Such data is not siloed by the customer; the CBDC ledger would show the entire financial web of transactions from customer to customer—thus providing a perfect, up-to-date ledger of CBDC ownership and history for all customers.[157] This three-dimensional data is not contemplated within the GLBA's definition of "nonpublic personal information."[158] To adequately safeguard such data, Congress should amend the GLBA to more explicitly define protected data to include that which would be collected in the routine course of CBDC use.[159] To the extent that the FRS engages with this data, the GLBA also should be amended to explicitly incorporate the FRS as a financial institution, and the FRS should in turn work to develop the institutional competence and tools necessary to adequately safeguard consumer data.[160]

The FRS, for its part, denies that it would collect data in issuing a CBDC.[161] They instead point to an intermediated model, which would allow the FRS to issue CBDC funds to commercial banks, who in turn would offer "accounts or digital wallets" to users to "facilitate the management of CBDC holdings and payments."[162] However, this argument misses the mark for two reasons. First, a CBDC would necessarily be built on a centralized blockchain managed by FRS.[163] Although commercial bank accounts could facilitate the *management* of CBDC holdings and payments, the underlying financial data—who owns what at any given moment—would be stored *at and by* the FRS.[164] Commercial banks, bound as they are by anti-money-laundering and data privacy laws, would still be required to collect the same information to open a CBDC account as they would for any other bank account: the status quo.[165] Yet, the FRS would maintain control over the bulk of financial data inherent in the CBDC system: a dramatic departure from the status quo unaddressed by the FRS.[166]

---

156. *See* Van Niekerk, *supra* note 4; Soubouti, *supra* note 15, at 534–35.

157. *See* Van Niekerk, *supra* note 4 (stating that a CBDC could "[b]e tracked across every movement, where the account that is credited appends that information to the digital dollar, in perpetuity" and "[b]e stopped, returned to the source, returned to the previous account, or even destroyed at any moment.").

158. *See* Soubouti, *supra* note 15, at 534–35. The data is three-dimensional in the sense that for a single transaction, the data could show the relationship between the FRS and each party to the transaction, the relationship between parties to the transaction itself, and the relationships between each party to the transaction and all third parties with whom parties have transacted leading up to the transaction being examined. *Id.*

159. *See* Bock, *supra* note 131, at 326. The FRS has indicated that they will not implement a CBDC without direct authorization and support from Congress. *See* MONEY AND PAYMENTS, *supra* note 13, at 3 ("The Federal Reserve does not intend to proceed with issuance of a CBDC without clear support from the executive branch and from Congress, ideally in the form of a specific authorizing law."). Accordingly, any such authorization should include, as part and parcel, adequate data privacy standards in the form of a modification to the GLBA.

160. *See, e.g.*, Van Niekerk, *supra* note 4.

161. *See* MONEY AND PAYMENTS, supra note 13, at 13–14.

162. *Id.*

163. *See* Van Niekerk, *supra* note 4.

164. *See id.*

165. *See* MONEY AND PAYMENTS, *supra* note 13, at 19.

166. *See* Van Niekerk, *supra* note 4.; MONEY AND PAYMENTS, *supra* note 13, at 19.

Second, this argument ignores the fact that CBDC funds would operate in direct competition with commercial bank funds.[167] Commercial banks have no financial incentive to offer access (by extending credit options or otherwise) to a digital cash system that would reduce their profitability by funneling activity away from their own online transaction services.[168] To solve this issue, either some additional incentive would need to be provided to commercial banks to provide access to CBDC accounts for users, or the federal government (likely the FRS as owner of the CBDC system, network, and protocol) would need to step in to provide public access to consumers interested in opening a CBDC account.[169] Assuming that CBDC is legal tender, all businesses would have to accept CBDC funds and would therefore need a CBDC account, requiring the FRS to quickly develop the capability to handle millions of accounts.[170]

B. Solutions to Protect Consumer Data Privacy Include Commercial Bank Incentives, FRS Reform, and Legislation to Expand the Gramm-Leach-Bliley Act

To ensure that consumer data privacy is adequately safeguarded, there are three potential solutions.[171] First, a CBDC should be designed to incentivize commercial banks to make available CBDC accounts.[172] In an intermediated system, such as that proposed by the FRS in their *Money and Payments* paper, bank provision of CBDC accounts would not represent a significant expansion in data collected by such banks; commercial banks already collect this data routinely.[173] However, as discussed above, banks have little incentive to provide accounts that act in direct competition with

167. *See* MONEY AND PAYMENTS, *supra* note 13, at 17.

168. *See id.*; *see also* Van Niekerk, *supra* note 4.

169. *See* MONEY AND PAYMENTS, *supra* note 13, at 17 (also stating the risk of increased use of stablecoins in lieu of CBDC if such accounts are not generally available).

170. *See* James B. Thayer, *Legal Tender*, 1 HARV. L. REV. 73, 73 (1887) (discussing the history of legal tender at the foundation of our country, which strongly mirrors the debate over whether the FRS may issue a CBDC); *see also* Jess Cheng & Joseph Torregrossa, *A Lawyer's Perspective on U.S. System Payment Evolution and Money in the Digital Age*, BD. OF GOVERNORS OF THE FED. RSRV. SYS. (Feb. 4, 2022), https://www.federalreserve.gov/econres/notes/feds-notes/a-lawyers-perspective-on-us-payment-system-evolution-and-money-in-the-digital-age-20220204.htm [https://perma.cc/EJL6-TCGD] (detailing the differences between a Federal Reserve note and a bank deposit, including the ability for commercial banks to "affect the total stock of money through lending activities that credit the accounts of borrowers" and "expose[] their balance sheet to risk.").

171. The following solutions are mutually exclusive but not collectively exhaustive. All three should be pursued in order to mitigate the data privacy risks inherent in a CBDC. However, it may be the case that additional solutions recommend themselves as the issues surrounding a CBDC in the United States are further studied through additional research and scholarship.

172. *E.g.*, MONEY AND PAYMENTS, *supra* note 13, at 17.

173. *See* Bock, *supra* note 131, at 315.

commercial bank funds.[174] Such incentives could take many forms: for example, there could be significant demand for user accounts, which could provide an incentive for commercial banks to offer CBDC accounts as a means for capturing greater market share.[175] Alternatively, Congress could provide monetary incentive for banks to offer user accounts, or a U.S. CBDC could be designed with the goal of ensuring "little to no disruption to the banking sector."[176]

Second, the FRS should begin to develop the institutional competence to safeguard consumer data. Such data could be limited to the underlying financial data inherent in a CBDC (i.e., the entire web of transactions).[177] However, if commercial banks are unwilling to offer CBDC accounts, this data could include the same types of data that are currently collected by banks and other financial institutions *in addition to* the underlying financial data inherent in a CBDC.[178] Beyond the protection of data, absent an intermediated system in which commercial banks offer user accounts, the FRS would need to develop infrastructure to support customers, which would likely include a variety of support services such as customer service centers, technical support, and other auxiliary support mechanisms.[179]

Third, the GLBA should be expanded to explicitly cover both the types of data that would be collected with a CBDC and the federal institutions involved in issuing and managing the data underpinning the CBDC system.[180] Whether or not an intermediated system is used to issue CBDC funds, the Federal Reserve would, as discussed above, maintain financial data showing every transaction on the CBDC system and could theoretically combine that data with personally identifiable information provided by consumers in opening a CBDC wallet or account.[181] These three-dimensional financial data types are not considered in the GLBA or other federal data privacy laws—a

174. *See* MONEY AND PAYMENTS, *supra* note 13, at 17; *see also* Van Niekerk, *supra* note 4.

175. *See* Jess Cheng et al., *Preconditions for a General-Purpose Central Bank Digital Currency*, BD. GOVERNORS FED. RSRV. SYS. (Feb. 24, 2021), https://www.federalreserve.gov/econres/notes/feds-notes/preconditions-for-a-general-purpose-central-bank-digital-currency-20210224.htm [https://perma.cc/2D5U-U3Q3].

176. *Id.*

177. *See* Van Niekerk, *supra* note 4.

178. *See id.*; *CBDC vs Cryptocurrency*, *supra* note 2.

179. Little scholarship addresses the point of developing institutional competence to handle such massive amounts of financial data. However, these competencies likely exist across government (e.g., financial data managed and stored by the IRS, or customer support call centers at GSA) from which the FRS could extract best practices in data management and customer support. Further research should be done to assess the technical and logistical requirements necessary to implement a CBDC, with care taken to identify the competencies that can reasonably be leveraged from across government.

180. *See, e.g.*, Bock, *supra* note 131, at 326.

181. *See* Van Niekerk, *supra* note 4; MONEY AND PAYMENTS, *supra* note 13, at 19.

gap that must be addressed prior to the development and implementation of a CBDC system.[182]

V. CONCLUSION

A central bank digital currency represents a substantial opportunity to "fundamentally change the structure of the U.S. financial system" to make it more equitable, accessible, and responsive to a modern and increasingly digital world.[183] A CBDC would bring the U.S. dollar into the modern world and ensure the longevity of the dollar's international role.[184] However, a CBDC brings inherent data privacy risks that are not considered under current federal data privacy laws; consumer identity would be linked to every single transaction made, offering a complete big data picture of the entire digital financial system.[185] An expansion of the GLBA to explicitly include the types of data that would be collected by a CBDC system, including underlying financial information that would comprise the CBDC blockchain, is necessary to ensure adequate safeguards for consumer data. As the Federal Reserve System continues to seek feedback on CBDC, more research is needed to further examine potential data privacy risks.[186]

182. *See, e.g.*, Soubouti, *supra* note 15, at 534–35 (discussing types of data that are not considered within the framework of the GLBA).

183. MONEY AND PAYMENTS, *supra* note 13, at 17.

184. *See id.*

185. *See* Van Niekerk, *supra* note 4.

186. *See* MONEY AND PAYMENTS, *supra* note 13, at 21 (indicating that "[t]he Federal Reserve will only take further steps toward developing a CBDC if research points to benefits for households, businesses, and the economy overall that exceed the downside risks, and indicates that CBDC is superior to alternative methods."). It remains to be seen whether the United States will officially determine whether to pursue development of a CBDC, and such an effort would likely take years to implement.