Renita Marcellin - Senior Policy Analyst at Americans for Financial Reform
Written Testimony
U.S. House of Representatives - House Financial Services Committee
Task Force on Financial Technology Hearing: *"What's in Your Digital Wallet? A Review of Recent Trends in Mobile Banking and Payments"*

Thank you and good afternoon Chair Lynch, Ranking Member Davidson, and members of the taskforce and Committee. I am the daughter of immigrants who previously relied on susus–a rotating savings arrangement formed by a small group of peers– because of their limited access to the traditional banking system when they first entered the US. As a result, I am supportive of technology and financial firms that truly seek to expand financial inclusion, especially among marginalized and BIPOC communities. However, novel technology–such as digital wallets or mobile payments–and claims of financial inclusion are reasons why we should ensure there are adequate regulatory safeguards. The novelty of these tools means we do not fully yet understand their effects on our broader financial system. Additionally, it is yet unclear if these financial technology firms indeed expand financial inclusion to unbanked and marginalized communities. More importantly, if these firms achieve greater financial access, their failure will also disproportionately harm the same communities they aim to serve–the groups that have historically suffered the most from predatory and extractive financial products.

Thus there is a responsibility to proceed with caution and prudently examine claims of financial inclusion to avoid repeats of history–subprime mortgages were also once heralded as a means to expand homeownership to immigrant and low-income communities.[1] Furthermore, policymakers should ensure there are sufficient safeguards to protect consumers from fraud and erroneous transactions, abusive data collection, and companies flexing their increased market power as more large technology firms enter the financial services industry.

Financial Inclusion
The primary challenges to the claim that digital wallets in their current form will increase financial access are two-fold. First, they are account-based.[2] A transactional account usually acts as the funding source for the corresponding payment being made or the place to which funds are credited. Apart from design limitations, unbanked consumers tend to have lower household income than those with bank accounts, and are most often paid with paper checks.[3] But without a bank account and access to a debit card, converting that cash for use on mobile platforms and digital wallets is particularly difficult and costly. According to Professor Mehrsa Baradaran, the average unbanked person loses about ten percent of their total income to alternative financial service providers just to use their own money.[4]

---

[1] Remarks made by Former Federal Reserve Chair Alan Greenspan on Consumer Finance. April 2005.
[2] Federal Reserve Bank of Atlanta's Policy Hub. "Digital Currency, Digital Payments, and the 'Last Mile' to the Unbanked." August 2021.
[3] 2017 FDIC National Survey of Unbanked and Underbanked Households. Pg. 13.
[4] Testimony of Professor Mehrsa Baradaran before United States House of Representatives: Committee on Financial Services Task Force on Financial Technology. June 2020. Pg. 1.

The second limitation to greater financial inclusion is that most digital wallets are app based and thus require a smartphone.[5] According to the Pew Research Center, more than 80 percent of users connect a bank account, credit, or debit card to an app. Additionally, although four in five unbanked consumers own a smartphone, they are more likely than people who have their accounts canceled or suspended their cell phone service for cost reasons, thus limiting their ability to use mobile payments.[6]

These flaws are reflected in the user data. Unbanked households, households earning less than $60,000 per year, and individuals without a college degree use mobile payments at a significantly lower rate than others. Approximately, 58 percent of banked households have used mobile payments compared to 37 percent of unbanked households. 48 percent of individuals earning less than $60,000 use mobile payments compared to 62 percent for individuals earning more than $60k. And only 45 percent of individuals with a high school diploma use mobile payments compared to 63 percent of individuals with at least some level of college education.[7]

For these reasons, a recent paper by researchers at the Federal Reserve Bank of Atlanta, suggested that a more effective approach to increasing financial inclusion could be giving cash users access to digital payment vehicles that do not necessarily depend on traditional bank accounts.[8] This is one the goals of the newly introduced E-Cash bill sponsored by Chair Lynch. Similar proposals have been implemented successfully in Kenya and the Bahamas, the M-Pesa and the Bahamian Digital Dollar, respectively.[9] While policymakers should continue advocating policies that would expand banking access such as postal banking, providing alternative means of payments for the many households who still rely solely on cash, many of whom are lower-income and communities of color, should remain a paramount concern to lawmakers.

Consumer Protection - Fraud

In addition to financial inclusion concerns, the rise of digital wallets presents unique challenges to consumer protection. A recent New York Times report showed how banks fail to provide their customers any recourse when they are victims of scams or fraud schemes using Zelle or other person-to-person (P2P) apps.[10] The same quality–instantaneousness–that makes digital wallets a favorite among consumers, including myself, is also why it is widely used by scammers.

Reports of fraud are highly common and increasing. The CFPB received 9,277 complaints in the product category of "mobile or digital wallet" since it began accepting such complaints in 2017,

---

[5] Bostic, Raphael, Shari Bower, Oz Shy, Larry Wall, and Jessica Washington. Digital payments and the Path to Financial Inclusion. Federal Reserve Bank of Atlanta. 2020. Footnote 30 on pg. 18

[6] The Pew Charitable Trusts. "Can Regulators Foster Financial Innovation and Preserve Consumer Protections?" Sept. 2020.

[7] Id.

[8] *Supra* note 2.

[9] id

[10] Stacy Cowley and Lananh Nguyen. "Fraud Is Flourishing on Zelle. The Banks Say It's Not Their Problem." March 2022.

through April of 2021.[11] Complaint volume has steadily increased over time. In 2017, the CFPB received more than 1,000 complaints about digital wallets. Between April 2020-April 2021, the CFPB received more than 5,200 complaints. Then in April 2021 alone, there were 970 digital wallet complaints.[12] The three most common complaints involving digital wallets are problems managing, opening or closing accounts; problems with fraud or scams; and problems with transactions (including unauthorized transactions). PayPal (which owns Venmo), Square (which owns Cash App) and Coinbase accounted for more than two-thirds of all digital wallet complaints through April 2021.[13]

Customers frequently lack recourse when problems arise with their digital wallets. Customer service for payment apps is minimal, sometimes lacking contact phone numbers or human interaction at all.[14] Consumers with a dispute were twice as likely to say it was difficult to resolve compared with people who had debit, credit, or general purpose reloadable (GPR) prepaid card transaction issues (39% vs. 20%).[15] They were also more than four times as likely as traditional payment users to not know whom to contact (23% vs. 5%).[16] With a traditional plastic card, it is very clear who the consumer should contact regarding an error. With a digital wallet, it is less clear. As Professor Adam Levitin highlights in his 2018 paper, would a consumer who had an error while using their Chase Visa card via ApplePay contact Chase or Applepay?[17] The confusion can lead to a delay in reporting, which then affects the consumer liability for the error. Currently, if an unauthorized electronic transfer is not reported within sixty days of receiving a statement, the financial institution is not required to reimburse the consumer.[18] Thus inadequate customer services on the digital wallet's end or lack of clear information regarding error resolution can be costly to the consumer.

Legal and Regulatory Framework

Besides the lack of customer service, consumers who use digital wallets will also find their legal options to remedy fraud and erroneous transactions are confusing and tedious. Different regulations govern each of the popular payment methods. Credit card transactions are governed by the Truth in Lending Act and Regulation Z; debit card transactions by the Electronic Fund Transfer Act and Regulation E; and Automated Clearing House transactions–transfers done using a bank's routing number– are governed by the National Automated Clearinghouse Association (NACHA) private rules. These myriad of laws do not adequately protect consumers using digital wallets from fraud and erroneous transactions.

Digital wallets are usually linked to one or a combination of these three funding sources. For

---

[11] Consumer Financial Protection Bureau, Consumer Complaint Database, with date counter set to 4/1/2017--5/1/2021.
[12] U.S. PIRG Education Fund. "Virtual Wallets. Real Complaints." June 2021. Pg. 2.
[13] *Id.* Pg. 4
[14] Luke Wilson."Cash App fraud up over 300% — what you need to know." Tom's Guide. March 2021.
[15] The Pew Charitable Trusts. "Are Americans Embracing Mobile Payments?" Oct. 2019. Pgs. 14-16.
[16] *Id.*
[17] Professor Adam Levitin. "Pandora's Digital Box: The Promise and Perils of Digital Wallets." University of Pennsylvania Law Review. Jan 2018. Pg. 339
[18] 15 U.S.C. § 1693g(a)(2) (2012)

example, for credit card consumers their unauthorized transaction liability is capped at $50[19]; for debit cards it varies between $50, $500, and unlimited liability, depending on the consumer's negligence[20]; and under NACHA rules there is no consumer liability for unauthorized transactions.[21] Thus, the consumer may have varying levels of protection depending on which source of funding was linked to the transaction. This is particularly concerning given that many types of digital wallets auto-default to a specific linked card or automatically change the card selected by the consumer if there was a problem with the initial payment method.[22] This problem does not exist with physical wallets because customers are very clear which card is being given for payment.

Additionally, payments that consumers are fraudulently induced to send fall outside of the definition of "unauthorized charge."[23] Banks claim that Regulation E only requires them to cover "unauthorized" transactions; however, many of the now popular scams involve inducing the customer to authorize a transaction by posing as someone familiar or a bank official.[24] Furthermore, banks are not required to publicly report their losses or aggregate reports of fraud.[25]

Customers currently have very little redress if a financial institution freezes an account because it spots red flags of fraudulent use or identity theft. Currently, it is not clear how long the freeze may last or what rights consumers have if they believe their account was wrongfully frozen.[26] Lastly, I would be remiss if I did not add that many of the major players in the digital wallet space that allow consumers to maintain a balance, for example Venmo and PayPal, are not FDIC insured.[27] Thus in the event of their bankruptcy, consumers have little, if any, recourse to recover their money.

Data Privacy Concerns

No single law provides a framework for regulating data privacy in the United States. Instead, myriad laws cover different industries. For the financial services industry, the main law governing privacy disclosures and implementing security standards is the Gramm-Leach-Bliley Act (GLBA).[28] It directs financial regulators to implement disclosure requirements and security measures to safeguard private information. And even the supervisory and rulemaking authority under GLBA is fragmented among the various banking agencies, the CFPB, and the FTC.[29] Furthermore, some interpret this law as being primarily applicable to traditional financial institutions. Many providers of digital wallets are tech companies.

---

[19] § 1643(a)(1)(B); 12 C.F.R. § 1026.12(b)(1)(ii) (2017).
[20] § 1693g(a); 12 C.F.R. § 1005.6(b) (2017).
[21] 2013 NACHA Operating Rules and Guidelines.
[22] *Supra* note 16. Pg. 337
[23] Advocacy Groups Comment Letter in Response to CFPB's Inquiry into Big Tech Payment Platforms. Dec 2021.
[24] *Supra* note 9
[25] *Supra* note 22
[26] *Id.*
[27] Ben Gran and Mitch Strohm. "Can PayPal Serve As Your Bank Account?" July 2021.
[28] CRS Report. "Big Data in Financial Services: Privacy and Security Regulation" Nov 2019.
[29] Id.

This dynamic also raises another gap in GLBA. It covers only nonpublic personal information held by financial institutions significantly engaged in financial activities. Technology firms that offer digital wallets are able to combine their aggregated consumer transaction data–a key difference with physical card payments–with consumer's past web browsing and geolocation.[30] Additionally, technology firms– who often sell consumer data–can compile public and private data from different sources that together reveal financially sensitive information.[31] This practice is not covered under GLBA. Furthermore, consumers have a limited ability to know, control, or correct financial data, which can make it difficult to obtain redress for violations such as data breaches. Section 1033 of the Dodd-Frank Act grants consumers the right to access information about their financial accounts, and requires any company or individual offering financial services to provide it.[32] But rulemaking under this statute has not yet been completed.

Anticompetitive Effects & Systemic Risk Concerns

The emergence of digital wallets as a tool for payments–particularly when those wallets are hosted by major technology firms or dominant retail businesses–also raises questions about economic concentration and anti competitive practices. By hosting digital wallets, these firms can leverage their market share and penetration across retail markets to offer their customers a variety of attractive features for payment schemes.

However, this same leverage can be abused in ways that unfairly constrain consumers' choices, increase costs for consumers due to monopoly control, exploit data collected from consumers via these wallets, or introduce systemic risk or instability. The Bank of International Settlements, in its 2019 Annual Report, described some of these risks in more detail, saying "Dominant platforms can consolidate their position by raising entry barriers. They can exploit their market power and network externalities to increase user switching costs or exclude potential competitors."[33]

Should a company issuing a wallet achieve scale rapidly and employ these anticompetitive practices, only to face volatility or a failure of its payment system, a large swath of the economy could be exposed to knock-on systemic risks and damage as a result. The President's Working Group on Stablecoins came to similar conclusions with respect to the systemic risks posed by custodial wallets provided by stablecoin issuers.[34]

Congress has acted in the past to address these concerns when it has come to more traditional payment systems. Historically, the Glass-Steagall Act was originally passed to cordon off financial services from commercial business activities in order to prevent these types of problems from occurring. More recently, the Dodd-Frank Act enabled payments systems to be designated as systemically important and subject to prudential regulation and oversight. Lastly, Congress and

---

[30] Cf. Privacy, GOOGLE, (describing how Google collects data from its users, including their websites browsed, locations visited, and videos watched).

[31] Brian Naylor. "Firms Are Buying, Sharing Your Online Info. What Can You Do About It?" NPR. July 2016.

[32] *Supra* note 27

[33] Bank for International Settlements. "Big tech in finance: opportunities and risks." June 2019.

[34] President's Working Group. Report on Stablecoins. Nov 2021.

federal regulators were quick to act when Meta proposed its Diem stablecoin as a payment system, recognizing the proposal as a well-consolidated example of all the risks described above.

As more major tech firms continue to expand into payment systems, monopolistic practices by wallet issuers are likely to persist unless or until more robust safeguards are enacted, either within the financial regulatory policy space, antitrust space, or some combination of the two. We urge regulators to consider using their authority under section 21(a)(2) of the Glass-Steagall Act and Title VIII of Dodd-Frank to discourage firms from illegally holding deposit liabilities and to ensure payment providers are not creating new systemic risk concerns.[35]

Policy Recommendations

To address the topics discussed above, Americans for Financial Reform propose the following regulatory and legislative recommendations.

Regulatory Recommendations

We urge the CFPB to take the following steps:

1) **Clarify that institutions have an existing obligation under the EFTA to investigate and resolve consumer errors in peer-to-peer (P2P) systems.** There are no limitations in the definition of "error" that bars institutions from considering errors made by the consumers [36] Indeed, the EFTA generally protects consumers even in situations when they are negligent. If a payment is made in error -- whether to the wrong person or in the wrong amount -- it does not matter who made the error; the recipient is not entitled to that payment, and it should be reversed. Thus, institutions should be complying with their duty to investigate and resolve errors.

2) **Expand the definition of "errors" under EFTA's rulemaking authority to ensure consumers using P2P services are protected from scammers who induce payments.**[37] Payments that consumers are fraudulently induced to send fall outside of the definition of "unauthorized charge; however, fraudulently induced payments can, and should, be considered an error triggering a duty to investigate and resolve the error. A payment that was sent to an imposter or under other situations involving fraud can and should be deemed an error.

3) **Clarify the rules and protections when accounts are frozen**. While we understand the need to stop fraudulent charges on an account, we urge the CFPB to consider the impact of a frozen account to consumers whose accounts were incorrectly frozen. Consumers

---

[35] 12 U.S.C. 378 Section 21(a)(2) and Dodd-Frank Title VIII

[36] Acts constituting an "error" include "an incorrect electronic fund transfer from or to the consumer's account." 15 U.S.C. § 1693f(f)(2); *see* 12 C.F.R. 1005.11(a)(2)(ii) (same). Nothing in the statute, regulations or official comments requires that the error be one made by the financial institution.

[37] 15 U.S.C. § 1693f(f)(7).

should have the right to contest a frozen account as an error under the EFTA (because the freeze will prevent the correct debiting and crediting of electronic fund transfers), and that error resolution procedures should apply.

4) **With respect to data sharing issues, clarify the application of existing federal data governance laws, including GLBA and the Fair Credit Reporting Act (FCRA).** A P2P payment system is certainly a "financial institution" under GLBA because payment processing is a "financial activity as described in" the Bank Holding Act.[38] Thus, any sharing of information with third parties is subject to the privacy notice requirements under Regulation P and the P2P company is subject to the data security requirements of the Federal Trade Commission's Safeguards Rule. To the extent that the P2P company sells or shares information to a third party, it could fall within the purview of the FCRA, or even a consumer reporting agency if the information is not first-hand experience information and the third party uses it for credit, employment or other FCRA-covered purpose.

In addition to the CFPB, we urge the Department of Justice to use its authority under section 21(a)(2) of the Glass-Steagall Act to determine if non-bank firms are illegally taking deposits. We also ask the FSOC to evaluate the systemic risks created by digital wallets and P2P platforms and use its appropriate authorities under Title VIII of Dodd-Frank to mitigate such risks.

Legislative Recommendations

We urge representatives to co-sponsor and support Chair Lynch's Electronic Currency and Secure Hardware (ECASH) Act (H.R. 7231) and the Protecting Consumers From Payment Scams Act, the legislation that has been noticed as part of this hearing. We believe solving many of the issues discussed above require vigilance by both regulators and legislators. We look forward to working with your staff to pass these important pieces of legislation. Thank you for your time and the opportunity to speak before you today.

[38] 15 U.S.C. § 6809(3)(A) (referring to 12 U.S.C. § 1843(k)); 12 C.F.R. § 1016.3(l)(1). Note that 12 U.S.C. § 1843(k) states at paragraph 4 "the following activities shall be considered to be financial in nature: (A) Lending, exchanging, *transferring*, investing for others, or safeguarding *money* or securities." (emphasis added). *See* 15 U.S.C. §1693a(12)