WHAT'S IN YOUR DIGITAL WALLET? A REVIEW OF RECENT TRENDS IN MOBILE BANKING AND PAYMENTS

HYBRID HEARING

BEFORE THE

TASK FORCE ON FINANCIAL TECHNOLOGY

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

APRIL 28, 2022

Printed for the use of the Committee on Financial Services

Serial No. 117–82

U.S. GOVERNMENT PUBLISHING OFFICE
47–649 PDF WASHINGTON : 2022

HOUSE COMMITTEE ON FINANCIAL SERVICES

MAXINE WATERS, California, *Chairwoman*

CAROLYN B. MALONEY, New York
NYDIA M. VELÁZQUEZ, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
DAVID SCOTT, Georgia
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
ED PERLMUTTER, Colorado
JIM A. HIMES, Connecticut
BILL FOSTER, Illinois
JOYCE BEATTY, Ohio
JUAN VARGAS, California
JOSH GOTTHEIMER, New Jersey
VICENTE GONZALEZ, Texas
AL LAWSON, Florida
MICHAEL SAN NICOLAS, Guam
CINDY AXNE, Iowa
SEAN CASTEN, Illinois
AYANNA PRESSLEY, Massachusetts
RITCHIE TORRES, New York
STEPHEN F. LYNCH, Massachusetts
ALMA ADAMS, North Carolina
RASHIDA TLAIB, Michigan
MADELEINE DEAN, Pennsylvania
ALEXANDRIA OCASIO-CORTEZ, New York
JESÚS "CHUY" GARCIA, Illinois
SYLVIA GARCIA, Texas
NIKEMA WILLIAMS, Georgia
JAKE AUCHINCLOSS, Massachusetts

PATRICK MCHENRY, North Carolina, *Ranking Member*
FRANK D. LUCAS, Oklahoma
BILL POSEY, Florida
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
ANN WAGNER, Missouri
ANDY BARR, Kentucky
ROGER WILLIAMS, Texas
FRENCH HILL, Arkansas
TOM EMMER, Minnesota
LEE M. ZELDIN, New York
BARRY LOUDERMILK, Georgia
ALEXANDER X. MOONEY, West Virginia
WARREN DAVIDSON, Ohio
TED BUDD, North Carolina
DAVID KUSTOFF, Tennessee
TREY HOLLINGSWORTH, Indiana
ANTHONY GONZALEZ, Ohio
JOHN ROSE, Tennessee
BRYAN STEIL, Wisconsin
LANCE GOODEN, Texas
WILLIAM TIMMONS, South Carolina
VAN TAYLOR, Texas
PETE SESSIONS, Texas

CHARLA OUERTATANI, *Staff Director*

TASK FORCE ON FINANCIAL TECHNOLOGY

STEPHEN F. LYNCH, Massachusetts, *Chairman*

JIM A. HIMES, Connecticut
JOSH GOTTHEIMER, New Jersey
AL LAWSON, Florida
MICHAEL SAN NICOLAS, Guam
RITCHIE TORRES, New York
NIKEMA WILLIAMS, Georgia

WARREN DAVIDSON, Ohio, *Ranking Member*
PETE SESSIONS, Texas
BLAINE LUETKEMEYER, Missouri
TOM EMMER, Minnesota
BRYAN STEIL, Wisconsin

CONTENTS

WITNESSES

THURSDAY, APRIL 28, 2022

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

WHAT'S IN YOUR DIGITAL WALLET? A REVIEW OF RECENT TRENDS IN MOBILE BANKING AND PAYMENTS

Thursday, April 28, 2022

U.S. HOUSE OF REPRESENTATIVES,
TASK FORCE ON FINANCIAL TECHNOLOGY,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The task force met, pursuant to notice, at 2:42 p.m., in room 2128, Rayburn House Office Building, Hon. Stephen F. Lynch [chairman of the task force] presiding.

Members present: Representatives Lynch, Himes, Lawson, Torres, Williams of Georgia; Davidson, Sessions, Luetkemeyer, and Steil.

Chairman LYNCH. Good afternoon. The Task Force on Financial Technology will now come to order.

Without objection, the Chair is authorized to declare a recess of the task force at any time. Also, without objection, members of the full Financial Services Committee who are not members of the task force are authorized to participate in today's hearing.

Today's hearing is entitled, "What's in Your Digital Wallet? A Review of Recent Trends in Mobile Banking and Payments."

I will now recognize myself for 5 minutes for an opening statement.

Digital wallets are software applications used to facilitate electronic payments and transactions and are rapidly becoming a larger part of our financial ecosystem. They are offered by a variety of players. Digital wallet providers range from large technology companies such as Google and Apple, to fintech companies such as PayPal and Block, and a consortium of banks which offer Zelle.

The digital wallet space has grown dramatically in recent years and reached a value of $120 billion in 2021. In addition to payment-focused digital wallets, we have seen the emergence of digital asset wallets which can hold cryptocurrencies and stablecoins. Digital wallets have grown in popularity, in part because of the ease and convenience that they offer, allowing individuals to send and receive money quickly with just the use of their phone. The use of digital wallets has also raised several key policy questions around consumer data privacy, security, and vulnerability to fraud.

Notably, according to a recent report, 18 million consumers were defrauded through scams involving digital wallets in 2020, and with the rate of adoption, that number is expected to increase. So, it is fair to ask whether consumers are unknowingly trading the

short-term ease and convenience of digital payments for the long-term loss of personal financial data and a latent vulnerability that could undermine their financial security. And as large technology companies enter the financial services space, how do we ensure that acquisition of personal data is limited and appropriate, and that both personal data and financial data are separate and secure?

From a consumer protection standpoint, the law remains unsettled as to how consumer protection laws apply to digital wallets, particularly in cases of fraud. The New York Times recently published an article that highlighted the major fraud issues involved with Zelle, which is a payment app created by America's largest banks and other payment platforms. The New York Times reported that Zelle had become a, "favorite of fraudsters," and that apparently, the major banks were reluctant to protect consumers who were unwittingly scammed using the platform application that the banks themselves had created. So, we are faced with the question, who should be on the hook when a consumer has been tricked into transferring their hard-earned savings by fraudulent online activity while transacting through digital wallets on an online banking platform?

To settle the regulatory ambiguities and to incentivize resiliency in digital commerce, the Protecting Consumers from Payment Scams Act, which is noticed with this hearing, would amend the Electronic Fund Transfer Act to protect consumers when they are defrauded into sending money by a scam, or even when the consumer was induced to make that payment under false pretenses. While proponents of digital wallets point to high adoption rates as evidence that digital wallets can promote financial inclusion, we should not ignore the fact that most financial products, including digital wallets, again, require a customer to have a bank account, which in the past has been shown to exclude a significant segment of consumers who will likely remain unbanked.

And lastly, as financial services move into the digital area, the war on cash continues to spread. As we shift towards digital commerce and away from physical cash, we leave behind a segment of consumers who rely on physical cash because they do not have access to digital products. These gaps continue to highlight the need for a public sector digital payment offering that allows for instant peer-to-peer (P2P) payments, and also protects consumer privacy. Consumers should not be required to surrender their personal data every time they make a simple financial transaction. That is the Chinese model, and it facilitates full-spectrum surveillance of the entire population, which is the reality toward which we are moving in this country.

To avoid that looming threat, I recently introduced the ECASH Act, which would direct Treasury to design and pilot a digital version of cash also known as ECASH. That bill progresses the conversation around digital dollar design and would work in parallel with other public sector digital offerings, such as the Fed-issued central bank digital currency (CBDC). ECASH would be distributed directly to and held by the public on a hardware secure device. It would allow individuals to make instant peer-to-peer payments with no consumer data or transaction tracking, and without the

use of a bank account. I hope that bill will work to address many of the challenges I described with digital wallets, and will have a strong financial inclusion implication. I look forward to discussing the policy questions associated with digital wallets and the potential benefits of a public sector offering with our witnesses.

I now recognize the ranking member of the task force, the gentleman from Ohio, Mr. Davidson, for an opening statement.

Mr. DAVIDSON. Thank you, Mr. Chairman, and I especially appreciate your emphasis on cash and how it is so vital for so many people in our economy. I always say the legal tender in the U.S. is the U.S. dollar, not Visa and MasterCard, and it is great because it is permissionless and the features include privacy. So, thanks again for your emphasis on privacy. I think it highlights that a lot of the topics that this FinTech Task Force have tackled are truly bipartisan. The growth in payment applications continues to drive the development of our digital economy, while fostering further innovation. I am glad this task force will again serve as a venue to gather the appropriate information needed to ensure that future policies in this space will not inappropriately hinder innovation.

As Congress contemplates a Federal standard for data privacy, we need to ensure that any future proposals in this space: one, will promote data minimization; two, are technology neutral; three, will prioritize informed choice and transparency amongst consumers; and four, will preempt State laws so that we have a national uniform standard for privacy. Abiding by these principles will protect liberties that have been in place long before these new payment systems were developed. And when I speak of this, I am alluding to the privacy protections that were embodied within cash transactions that existed long before we were even using electricity. The privacy concerns cannot be understated as we consider how to embrace these new payment tools.

I understand that some people here today will likely discuss the positive impact that digital payments will have on financial inclusion. However, I would emphasize that promoting convenience to the consumer does not always equate to promoting financial inclusion. For example, we already know that distrust in traditional financial institutions is one of the main reasons why some people remain unbanked or underbanked. This is largely because these entities serve as an arm of the government via third-party doctrine. They have essentially been deputized to serve as agents of the government. In 2019, the FDIC reported that 36 percent of unbanked individuals cited lack of trust in financial institutions as a reason that they remain disconnected from the banking system.

Therefore, if new digital payment systems look to promote financial inclusion, we must recognize that it will only happen if we are able to promote trust by protecting consumers from having their personal data exploited without their consent, or, in some circumstances, beyond their consent.

Now, as someone who talks regularly about cryptocurrency and blockchain applications, blockchain technology, when given the chance, I would be remiss, and everyone would surely be disappointed if I didn't mention the permissionless nature of the distributed ledger technology that alleviates privacy concerns because it establishes trust in a different way. As I am sure many are

aware, blockchain technology offers privacy protection and guarantees that traditional financial tools may not offer, even though they can serve a common or identical purpose.

Since the title of this hearing was published, I have had questions from many people. Does the term, "digital wallet," mean that this hearing will primarily focus on crypto? Well, I wish that it did focus more directly on crypto. But I mentioned this not to shift the focus of the hearing, which is a good topic as well, but to point out that the conversation today will inevitably lead to further discussion on true peer-to-peer permissionless transactions carried out through hardware wallets, self-custody on a permissionless distributed ledger technology architecture. And that is a conversation that I very much look forward to having with my colleagues in a comprehensive way, and on an adjacent bill, the Keep Your Coins Act, which protects self-custody.

But back to the focus of today's hearing, I think we will hear some repetition from our prior task force hearing back in the fall to discuss the CFPB's rulemaking under Section 1033 of the Dodd-Frank Act. Like many, I am curious as to how that rulemaking will look because it is important to adequately address data-sharing issues on the front end and back end of digital payments systems. It won't be until the Consumer Financial Protection Bureau (CFPB) moves forward with that final rule that we can actually see the digital payment space progress forward and provide further financial convenience to consumers in a responsible manner. Should the CFPB leave any open-ended questions with their final rulemaking, I would then welcome the opportunity to work with my colleagues on this committee to responsibly write legislation that puts consumers truly in control of their own data, while allowing the digital economy to flourish here in the United States.

I look forward to the hearing and the discussion with our witnesses. Thank you all for being here today, and I yield back.

Chairman LYNCH. The gentleman yields back. I do not see Mr. McHenry, but we will reserve time for him.

Today, we are fortunate to welcome the testimony of a panel of distinguished witnesses. First of all, we have Raul Carrillo, who is joining us remotely. Mr. Carrillo is an associate research scholar at Yale Law School, and the deputy director of the Law and Political Economy Project. He has also been enormously helpful to the committee, and to the task force, in drafting legislation, and we are grateful for his attendance here today.

Second, we have Mishi Choudhary, who is the legal director of the Software Freedom Law Center.

Third, we have Renita Marcellin, who is a senior policy analyst for Americans for Financial Reform.

Fourth, we have Kia McAllister-Young, who is the director of America Saves at the Consumer Federation of America.

And lastly, we have Scott Talbott, who is the senior vice president of government affairs for the Electronic Transactions Association.

Witnesses are reminded that their oral testimony will be limited to 5 minutes. You should be able to see a timer in front of you on your screen that will indicate how much time you have left, and there will also be a chime which will go off at the end of your time.

I would ask that you be mindful of the timer, and quickly wrap up your testimony if you hear that chime, so that we can respect the time of our witnesses and task force members.

And without objection, your written statements will be made a part of the record.

Mr. Carrillo, you are now recognized for 5 minutes to give an oral presentation of your testimony. Welcome.

STATEMENT OF RAUL CARRILLO, ASSOCIATE RESEARCH SCHOLAR, YALE LAW SCHOOL, AND DEPUTY DIRECTOR, LAW AND POLITICAL ECONOMY PROJECT

Mr. CARRILLO. Thank you, Chairman Lynch, Ranking Member Davidson, and members of the task force. I echo my previous remarks before this task force and the committee, urging policymakers to demand public accountability, but also public innovation. I will tab in my initial remarks to two sets of problems in the digital wallet space that must be overcome in order for us to have a safe and inclusive financial system. For simplicity's sake, I will call these two problems the banking problem and the data problem.

First, the banking problem. Many wallets are holding balances that are not insured by the FDIC. In cases where a pass-through insurance is provided, customers are protected against the collapse of a bank, but not necessarily a wallet provider or coin issuer. This can become an unstable situation. Deposits that are not regulated as such often form the base layer of financial crises. This is in part due to a nod in banking law. For instance, Section 21 of the Glass-Steagall Act makes it illegal for an entity to accept deposits without being regulated by a banking regulator.

Unfortunately, the Act has not defined, "deposit," meaning that regulators cannot easily invoke Section 21 or any other provision of Federal law to prevent nonbanks from engaging in general banking activities. I believe the recent White House memo on stablecoins makes strides in this direction, but that the Stablecoin Tethering and Bank Licensing Enforcement (STABLE) Act, cosponsored by Chairman Lynch, Representative Rashida Tlaib, and Representative Chuy Garcia, achieves these goals more comprehensively, including by reaching non-stablecoin wallets.

Second, the data problem. Fintech increasingly relies on data maximization, as both Chairman Lynch and Ranking Member Davidson indicated. Data maximization is a constant expansive accumulation of consumer data. New fintech products, like digital wallets, may generate helpful information, serving as gateways to saving credit and investment. However, they also operate within massive information networks, including consumer reporting agencies, specialty screening agencies, data brokers, and government agencies, which amplifies systemic security and privacy risks by compounding data, potentially creating a data ecosystem that is also too-big-to-fail. The risk of thefts, hacks, and surveillance are especially pronounced for low-income communities of color that already suffer disproportionately from financial injustices and privacy violations.

Unfortunately, no overarching Federal law structurally limits the collection, use, and sale of personal data among corporations. Moreover, there are few rules governing information sharing between

these institutions and the government. Case in point, it was recently revealed that for a period of over 2 years, the Department of Homeland Security collected records from Western Union for any money transfer over $500 to or from California, Texas, New Mexico, Arizona, and Mexico. I grew up on the border and find the fact that my community is not protected by the principles of the Fourth Amendment to be entirely unacceptable.

The nature of public-private surveillance should inform the way that we talk and think about financial inclusion. At this point, leading scholars of data governance, security, and privacy agree that laws on the books do not sufficiently protect consumers. Definitionally, our notice and consent laws cannot empower people to protect their privacy, because when people consent to share data, we don't know how it will be used or how it may help or harm others. A comprehensive CFPB in that rulemaking may offer one way forward.

Ultimately, however, Congress should pass legislation instantiating data minimization, including by limiting the collecting, processing, and usage of data to only that which is required to carry out an explicit, narrow, permissible purpose; otherwise, it is not allowed. For example, signing up for a credit card online should not lead to targeted advertising or new accounts regardless of whether one clicks, "I agree," to data usage policies that consumers do not understand and firms cannot and do not uphold.

Most importantly, I support legislation creating a digital dollar and digital public options for a wide array of products, including bank accounts for all. However, the new public system must also be attuned to data minimization. Accordingly, I strongly support the ECASH Act proposed by Chairman Lynch, which would aim to replicate the privacy, security, and financial inclusion functions of physical cash. ECASH would work on stored value devices, storing the money offline on hardware rather than online on software. This has distinct security, privacy, and financial inclusion advantages. The way it would work is, I would simply tap a card against another person's card, or a phone against another person's phone, or a phone or a card against a retail kiosk. The payment would initiate regardless of whether I have an internet connection, so long as the device has judged that there was no counterfeiting or other foul play.

Just like physical cash, ECASH would include its own security features and would not be used for every financial transaction. But it would: one, reach the 1 in 3 adults in the U.S. who lack high-speed internet access in their homes and often in their neighborhoods who are not reachable by private fintech; and two, preserve a space for financial privacy in the future.

In my humble opinion, we are now having a comprehensive national policy discussion about financial privacy for the first time since the Patriot Act. Now is the time for public accountability and public innovation rather than false promises and fear. Thank you.

[The prepared statement of Mr. Carrillo can be found on page 26 of the appendix.]

Chairman LYNCH. Thank you, Mr. Carrillo.

Ms. Choudhary, you are recognized for 5 minutes. Thank you.

STATEMENT OF MISHI CHOUDHARY, LEGAL DIRECTOR, SOFTWARE FREEDOM LAW CENTER

Ms. CHOUDHARY. Thank you, Chairman Lynch, Ranking Member Davidson, and distinguished members of the task force and the committee. I am pleased to appear before you today. I am the legal director of the New York-based Software Freedom Law Center.

One could not send or receive email, surf the World Wide Web, perform a Google search, or take advantage of many of the other benefits offered by the internet without free and open-source (FOSS) software. FOSS developers create and advance solutions to complex problems that are decentralized, open, and accessible to everyone. My last point today will concentrate on getting regulatory clarity, having an open source of the underlying tech interoperability, and the importance of comprehensive Federal privacy legislation.

What we need is a currency or an electronic token that is equivalent in functionality to cash, and offers all of its benefits, including anonymity, privacy, autonomy, no transaction fees, and addresses all of the flaws of cash. In a rapidly-evolving technological environment, you must seek payment methods that are convenient, inexpensive, and secure. Our legacy transaction systems have suffered from high fees, limited access, and modest innovation that has beset many financial inclusion efforts. Most of the current solutions available in the market cater to the bank customer and don't address those who primarily work in the informal economy or are paid in cash. That part of the American population also desires the modern conveniences that technology offers without losing their privacy.

The transition to digital payments was already underway, but the pandemic accelerated adoption to a new level. Despite a massive rate of adoption of these forms of payment, unlike the Chinese or the Indian market that are mobile first, the U.S. market still relies heavily on credit cards. A U.S. customer does not necessarily have the same motivation as their Indian or Chinese counterparts, especially because credit card systems are backed up by various laws like the Fair Credit Billing Act (FCBA), the Electronic Fund Transfer Act (EFTA), and the Credit Card Accountability Responsibility and Disclosure Act (Credit CARD Act). Non-traditional players in the market have attempted to address some of these issues through the use of mobile devices to improve access to financial products and services. Digital wallets are one such example. In general, they are linked to a bank account, a credit or debit card, or a prepaid card, but they don't have to be.

Cryptocurrencies, which are right now stored in hot and cold wallets—"hot" means that they are connected to the internet, and cold storage wallets do not require online servers and can store the assets in the wallet—offer an additional security layer. As we think about money in the age of the internet, we must design for a future that is in the public's interest, incorporates privacy by design, and facilitates financial inclusion.

The super apps that are popular in countries like China, and are gaining popularity around the world, underscore the fact that concerns about data protection and privacy have not been adequately addressed, and that the current market options lack privacy-ori-

ented messaging systems integrated with payments. We need a currency or electronic token that is equivalent in functionality to cash. Such a design finds support in the streets, as resonated by David Chaum in the 1990s, and recently-introduced electronic currency and secure hardware cash by Representative Lynch that directs Treasury to commence two stage pilot programs to test a variety of ECASH technologies.

The risks of hard money for working-class people have always been lost in convenience or inflation. Working people back to the Jacksonian era in the United States have much experience with various payment systems chosen by employers that have hurt them, so they favor hard money, government coins that are deep in the fabric of democratic finance in the United States. In the 21st Century, it should not matter whether what you are waving at the cash register is a card issued to you by a bank, or a credit union, or a hardware object that the United States Treasury has certified as the way that ECASH is carried around.

The structure of ECASH does not have the quality of traceability and it preserves privacy. The software underlying any of this technology must be free and open-source to enable public review and audit of the source for potential security issues. If used correctly, with adequate guardrails, digital money presents an opportunity for financial inclusion. Any such efforts must provide consumer protection and data privacy aspects, often found to be woefully lacking in several such offerings around the globe. What we need is to have multidisciplinary research in the development of technologies that work for those who are most disadvantaged by the current system, those who don't have bank accounts and have to pay high fees to access their own money, built with privacy by design.

Thank you for the opportunity to appear before you today, and I look forward to your questions.

[The prepared statement of Ms. Choudhary can be found on page 37 of the appendix.]

Chairman LYNCH. Thank you, Ms. Choudhary.

Ms. Marcellin, you are now recognized for 5 minutes to give an oral presentation of your testimony. Thank you.

STATEMENT OF RENITA MARCELLIN, SENIOR POLICY ANALYST, AMERICANS FOR FINANCIAL REFORM

Ms. MARCELLIN. Thank you, and good afternoon, Chairman Lynch, Ranking Member Davidson, and members of the task force.

As a daughter of immigrants who had limited access to the traditional banking system when they first entered the U.S. and supported their family abroad using remittances, I am supportive of technology and financial firms that truly seek to expand financial inclusion. However, the question is still open on whether these products actually expand financial access. And if we assume they do, their failure will disproportionately harm the very communities they aim to serve, hence why they need to be properly regulated. Policymakers should also 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.

It is hard to see how digital wallets promote financial inclusion when they are usually account- and app-based. They usually require the consumer to link the wallets to a bank account or credit card and a smartphone. Unbanked consumers tend to have lower household incomes than those with bank accounts, are often paid with paper checks, and spend about 10 percent of their income on services just to access their own money. Additionally, unbanked households are more likely to cancel or suspend their cellphone service for cost reasons, hence limiting their ability to use mobile payments.

The Federal Reserve Bank of Atlanta suggested a better way to increase financial inclusion, by giving people who depend on cash, access to digital payment methods that do not depend on traditional bank accounts. This is one of the goals of the newly-introduced ECASH bill sponsored by Chairman Lynch. While policymakers should continue pushing policies that would expand banking access, such as postal banking, they should still prioritize ensuring that those who rely on cash and remittances are able to transact in our modern economy, many of whom are lower-income communities of color.

Digital wallets do not adequately protect consumers. Many banks fail to provide their customer any recourse when they are victims of fraud schemes using Zelle or other peer-to-peer apps. The same quality instantaneousness that makes digital wallets a favorite among consumers, including myself, also makes it a favorite among scammers. The Consumer Financial Protection Bureau (CFPB) received over 9,000 complaints about digital wallets between 2017 and 2021. In April 2021 alone, there were almost 1,000 digital wallet complaints. PayPal, which owns Venmo, and Square, which owns Cash App and Coinbase, accounted for more than two-thirds of all digital wallet complaints through April 2021.

Customers frequently lack recourse when problems arise with their digital wallet. Many apps do not have a customer service number and lack any human touch points. This results in customers delaying reporting scams and can lead to consumers losing the right to be reimbursed. I go into much more detail in my written testimony on the current legal framework that governs digital wallets. But the basic point is that the myriad of existing laws do not adequately protect consumers when fraud or erroneous transactions occur. The definition of an, "unauthorized transaction," does not cover scams that induce the customer to send money or cases where the device was stolen. If this fraudulent transaction was linked to a debit card or claim, they are not required to reimburse the consumer.

In regards to privacy concerns, the main law governing privacy for financial institutions has gaps when we try to apply it to digital wallets. It is not currently interpreted to cover tech companies and only covers non-public personal information. Technology firms are able to combine consumers' transactional data with their browsing history. They can combine public and private information to reveal sensitive data about the consumer, all out of the consumer's control. Lastly, the emergence of digital wallets as a tool for payments,

particularly when those wallets are hosted by major technology firms, also raises questions about economic concentration and anti-competitive practices, which I urge the committee to further explore.

In my written testimony, I outlined numerous steps the CFPB can take to address erroneous and fraudulent transactions. We also urge Congress to pass the Protecting Consumers From Payments Scams Act, which will give the CFPB unquestioned legal authority to take the recommended measures.

Thank you for your time, and for the opportunity to speak before you today.

[The prepared statement of Ms. Marcellin can be found on page 41 of the appendix.]

Chairman LYNCH. Thank you, Ms. Marcellin.

Ms. McAllister-Young, you are recognized for 5 minutes for an oral presentation of your testimony. Thank you.

STATEMENT OF KIA MCALLISTER-YOUNG, DIRECTOR, AMERICA SAVES, CONSUMER FEDERATION OF AMERICA (CFA)

Ms. MCALLISTER-YOUNG. Chairman Lynch, Ranking Member Davidson, and members of the task force, it is an honor to be invited to testify and contribute to the ongoing conversation of digital wallets and mobile payment. My name is Kia McAllister-Young, and I am the director of America Saves, a national campaign that focuses on building financial stability, resilience, and confidence, particularly with low- to moderate-income earners, and supporting them in their quest to save successfully, reduce debt, and get on a path toward building wealth. America Saves is an initiative of the Consumer Federation of America (CFA).

My goal today is to highlight the consumer voice and experience that will hopefully add reverence and additional context for you while working toward policy and regulation. Experts agree, including my colleagues and advocates at CFA, that concerns about this topic include the high prevalence of fraud and scams, a lack of accountability, very few consumer protections beyond disclosures and warnings, ineffective consumer privacy, specifically around financial data privacy, and an overall need to strengthen Federal and State oversight.

My work at America Saves allows me to interface and engage on a continual basis with everyday consumers from all racial and socioeconomic backgrounds, many of whom are oblivious to the risks they are taking when using digital payment options like PayPal, Cash App, and Zelle, as opposed to cash, credit, and debit cards. Their choice to use these platforms is largely due to the convenience and honestly strategic marketing and placement. During the checkout process, consumers are presented with several different payment options, but are rarely as enthusiastically presented with the risks associated with those options. Consumers naturally trust these fintech platforms because a clear delineation between financial institutions and mobile payment applications does not exist. The result of that intentional opaqueness is consumers believing that mobile payment options are regulated with the same scrutiny as banks and credit unions.

Consumers' misguided trust of the fintech platform leaves them vulnerable to fraud, scams, and payments being held by the platforms with very limited and, at times, no recourse at all. In my written testimony, I shared my own experience of how PayPal held my funds for over 30 days back in 2018, and I have heard numerous similar stories through my work, like that of Lauren, who was a victim of fraud using PayPal that took over 8 months to find restitution, and Samira, a Muslim woman, an immigrant from Trinidad and Tobago, and a small business owner with several instances of her funds being held without clear cause.

The lack of clarity, consumer protections, and transparency is not evident to consumers until it is too late. Still, the use of fintech products has dramatically increased for two apparent reasons: public health; and inflation. Since the pandemic, these payment options have been heavily embraced as quick, available, and even safer ways to make transactions, and inflation is driving low- to moderate-income earners toward fintech credit products in order to access their pay early.

Other gaps that remain without more oversight and regulation include immigrant citizens who often send money back to their families and their native countries that are disproportionately subject to alarmingly high remittance fees, and the current trend of fintech platforms offering cryptocurrency rather than encouraging users to work toward achieving financial stability through saving for an emergency. Because the foundational motivations for use of mobile payment applications are not likely to change, the onus to protect consumers through education, transparency, policy, oversight, and regulation simply must be prioritized.

The good news is that these products can play a role in helping consumers manage their finances. But again, Federal and State oversight is needed to ensure consumers are protected from harmful practices and violations of data privacy. And as we work to rebuild our economy and increase financial resilience for every American, we must recognize and highlight what threatens our nation's ability to save, reduce debt, and build wealth. That work is an intersectional joint effort of financial education, along with policies and regulations that protect consumers from practices that make it hard to be fully informed.

Thank you for your time, and for the opportunity to share today.

[The prepared statement of Ms. McAllister-Young can be found on page 48 of the appendix.]

Chairman LYNCH. Thank you, Ms. McAllister-Young.

Mr. Talbott, you are now recognized for 5 minutes. Welcome.

STATEMENT OF SCOTT TALBOTT, SENIOR VICE PRESIDENT, GOVERNMENT AFFAIRS, ELECTRONIC TRANSACTIONS ASSOCIATION (ETA)

Mr. TALBOTT. Thank you. Good afternoon, Chairman Lynch, Ranking Member Davidson, and members of the Task Force on Financial Technology. I am Scott Talbott, and it is my privilege, as senior vice president of the Electronic Transactions Association (ETA), to speak with you today on how the modern payments industry is using the latest technology to provide secure, fast, and convenient payment services to consumers.

ETA is a trade association that represents the broad group of companies that provide electronic products and services, including mobile wallets, peer-to-peer (P2P) products, credit and debit cards, and other forms of digital payments. Ours is an industry that, in North America, moves over $8.5 trillion in card and P2P payments securely, reliably, and quickly. In the 5 minutes that I an testifying today, over 1.5 million consumer transactions will be processed. It is heavily regulated at both the Federal and State levels and highly competitive. We are constantly investing, innovating, and leveraging new technologies to create new products and services to serve the ever-changing needs of consumers.

Of all the developments in payments, I want to focus on two today, mobile wallets and P2P, which are two different products with different use cases, but many similarities. Mobile wallets, as has already been noted, is simply a platform to store payment credentials on your phone. Instead of reaching for a traditional plastic card or checkbook, consumers can contactlessly use cards stored in their wallets or in the mobile wallets in their phones to make purchases at stores and shop online. Mobile wallets make buying goods and services very convenient. Tourists can shop anytime, anywhere, with just a few clicks on their phone. Mobile wallets also benefit merchants by enhancing loyalty programs and, because of the speed of a sale, reducing transaction times.

Another innovation I would like to highlight is peer-to-peer apps, or P2P. P2P is largely a free and fast service designed primarily for the transfer of funds between family and friends in order to split the check at a restaurant, or send your grandkids some birthday money. P2P payments work by linking an individual's bank account and debit, credit, or prepaid card with a platform. For those consumers who do not have a bank account, we have solutions available as well. There are many options to allow cash-based consumers to load cash or paper checks onto their P2P wallets on their P2P services. Many retailers partner with P2P services to allow this to happen in locations across the country. P2P apps are very popular, used by tens of millions of consumers, and total transaction volumes are forecasted to reach close to $350 billion by the end of this year. And P2P offers similar ease of use and conveniences as digital wallets.

The two products, while different on the surface, are similar in many ways versus security. For the payments industry, security is a top priority. For all payment products, including mobile wallets and P2P apps, the payments industry employs a robust, holistic, and multi-level approach to security. A simple example of this is that the mobile phone itself requires a unique authentication to unlock, whether a PIN, a facial scan, or a fingerprint. Inside the phone, account numbers are not actually stored on the phone but rather use a token representing the account number, and the transactions are all encrypted, which means it can only be read by participants in the payments industry. By demonetizing the payment info, it is less attractive to see these.

Both products advance another top priority for the payments industry, namely financial inclusion. The digital wallets and P2P services can be used by cash-based consumers and accessed anytime. They help to advance this goal.

Lastly, both mobile wallets and P2P were instrumental during the pandemic. By partnering with the payments industry, the U.S. Treasury was able to electronically distribute billions of dollars in economic impact payments directly to millions of consumers' wallets and P2P accounts. Additionally, during the pandemic, contactless payments were helpful to eliminate the need for touching common services during checkouts.

This discussion just highlights some of the many innovations that are happening in the electronic payments industry. As I said, our members are investing billions of dollars annually to develop and deploy technologies that make it easier for individuals to accept, hold, and send or spend money securely, and we continue to integrate these ideas in technologies to make the current payment system safer and stronger.

One idea of what is next and what is new is crypto assets. As payments experts, ETA member companies are closely examining crypto space solutions to consider using payments space. While cryptocurrencies are predominantly used for investments at this point, once the policy framework is in place, ETA members will be able to widely deploy crypto for payments use cases. ETA has published guiding principles along these lines, and I look forward to working with the task force and Congress in general to advance good public policy in the crypto space.

On behalf of ETA member companies, I want to thank you again for the opportunity to participate and support this discussion, and I look forward to any questions you may have.

[The prepared statement of Mr. Talbott can be found on page 51 of the appendix.]

Chairman LYNCH. Thank you, Mr. Talbott. I will now recognize myself for 5 minutes for questions.

Mr. Carrillo, in your testimony, you describe how fintech business models often rely on data maximization, which is a term to describe the constant and expansive accumulation of consumer data, which leaves consumers vulnerable to fraud and exploitation. I have seen this in my own experience. You go online, and you are trying to buy something simple, like a pair of socks from a retailer, and you have to surrender your financial history and basically get naked with the retailer from a data standpoint in order to make a simple purchase, and it is infuriating sometimes, and there is no difference. They all seem to be trying to suck as much data out of the consumer as they possibly can.

I was wondering if you could discuss some of the issues that come with this level of data exposure and how public sector options—you could refer to the ECASH bill that you were so helpful on—provide the same convenience and ease of digital wallets without data exposure?

Mr. CARRILLO. Thank you very much, Chairman Lynch. I appreciate the question and also the invitation to speak about the bill. First, I would note that data maximization is the business model of many of these companies. And, in fact, they charge low fees or claim to charge low fees and have better conditions precisely because they collect data with virtually no limits, and this is not necessary for a simple payment, as you indicated. There are many cases in which I would prefer that the information from a payment

not be shared, and it is not because I am doing anything illegal, and that is the case for most people. It is simply that you do not need to surrender all of your information every time that you swipe or tap a card.

Now, ECASH brings us into the digital realm. But it reaches people who do not have an internet connection, first of all, but it also is usable by people who would prefer to have some space for privacy. The fact is that most of us use cash in some form. We also use debit cards. We use credit cards. We use Venmo. We use PayPal. And we know that each of those payment instruments entails different privacy and security features and accomplishes different functions. With the ECASH Act, we don't imagine that people are going to put their life savings on an ECASH wallet. But if we want to preserve a space for the financial privacy that has existed for thousands of years in the next financial upgrade, we need something like ECASH.

It may be the case one day that there are applications for something like a blockchain-based token, but the fact is when you put money on a ledger, it is, by definition, seeable by the people who operate that ledger. And when we talk about the blockchain, encryption may be involved, but we are also talking about data maximization in that sense as well. So, really to preserve this space, this inclusive private space within our payment system, we need to go offline. We need to go low-tech and provide this option, at the very least, for everyone. Thank you.

Chairman LYNCH. Thank you. Ms. Marcellin, you mentioned in your testimony about financial inclusion, and you raised the question of whether or not digital wallets are actually in fact achieving that financial inclusion.

Could you talk about some of the barriers that you see? It is a noble cause to obtain financial inclusion, but we are not there yet, and I am not sure if these digital wallets, as currently designed, offer that opportunity. But I would like to hear your perspective on that.

Ms. MARCELLIN. Yes, absolutely. Thank you for the question, Chairman Lynch. The FDIC, in a bank survey from 2019, I believe, estimated that about 5.4 percent of households in the United States are unbanked. And I believe the amount of Americans who use digital wallets or mobile payments is around 80 percent. It is very likely that most of those people—I am not going to say all—who are using these mobile apps are people who are banked, and I think some of the solutions are public banking options, so postal banking, the ECASH bill that has been raised. Also, even if we discuss remittances, the United States Postal Service (USPS) can expand the amount of countries to whom they offer remittances.

So, I still believe that there are a lot of digital wallets to go further on. People under $60,000, who make $60,000 annually, people who do not have college degrees, and, again, people who are unbanked, the data shows that they are not using it at the rates that people like myself are.

Chairman LYNCH. Thank you very much.

The Chair now recognizes the ranking member of the task force, the gentleman from Ohio, Mr. Davidson, for 5 minutes.

Mr. DAVIDSON. Thanks, again, Mr. Chairman, and, look, thank God that the American people aren't waiting for Congress to move forward with digital technology, right? They are way ahead of this hearing. People are doing this. It is not illegal to be doing it. There are people within the government who, frankly, want to try to make it illegal.

They are talking about essentially needing to get permission from the government. They even have self-custody for crypto, adding reporting requirements, including to IRS forms, and without real authorization to do it, frankly, with the IRS. And people operate and live their day-to-day lives in a digital world and they want to be able to move money digitally, and the technology is there to do it; we just don't have the legal clarity to help them.

And then, frankly, the consumer protections around privacy and data security likely do as was highlighted around payments with the safe credit cards. And people in the crypto space will recognize the basic default safety valve, not your keys, not your tokens, not your coins. But that has a huge hazard because people forget their passwords all day, every day, and if you forget your passwords to cold storage, well, they are gone, right? Those are high stakes.

So, I like that we are talking about something that for maybe less sophisticated customers, you have some of those protections, but we ought not try to eliminate the things that other people are already doing. We should put a good framework around those.

Mr. Talbott, let me start with you. As Congress contemplates a Federal standard for protecting consumer data privacy, it is important that any law can stand the test of time. And given the rate we are moving, how do we pull that off?

Mr. TALBOTT. Thank you, Ranking Member Davidson. In terms of privacy, a couple of ideas come to mind. First of all, we need a uniform national standard. It is very difficult for companies that operate across the country, with anyone with an internet connection, to comply with a patchwork of State privacy laws. We see this in other areas as well. So, first and foremost, would be a uniform national standard. Second, we want it to be principles-driven. Technology changes rapidly. The products and services that exist today didn't exist a couple of years ago, and there will be new products and services soon, so having a principles-based approach is key.

I think other areas or other concepts to think about within the space are control and transparency. This ties into a little bit of Section 1033 on open banking, gives them the ability to understand what is happening with the data, and to have control over it, which is key to any uniform national standard.

And then, one last point, is within the payment space, we largely do not see the SKU level data. We don't know that you are buying socks. We see the transaction, but we need to keep that data and then have a permissible right to use it to fight fraud. It is an important part of our fraud fighting efforts, and privacy laws should consider that along with other public policy goals like law enforcement going forward.

Mr. DAVIDSON. Yes, thank you. I think you touch on it, but don't really quite go there. And kind of in a separate bill that would be multi-jurisdictional, and I hope to call it H.R. 4, would restore the Fourth Amendment, which has been substantially eroded. We

should recognize a property right for people's data. Your personal identifiable information, your data, the content you create is really your property. It is your data, and we should be protecting that. I would say that would be the one principle that I would add, and without you verbalizing it, I think you get there. That is kind of where you are at. And as I highlighted, the market is way ahead of us; 69 percent of retailers now accept some form of contactless payment. Could you speak to how those innovations actually help small businesses and entrepreneurs?

Mr. TALBOTT. Sure. That's a great question. I think for small businesses, the ability to accept payments is crucial. Whether you just accept cash, you have to also accept payment cards, digital payments, and there is lots of competition and lots of options in the space. The fact that they can be loaded to your mobile wallet makes it easier for small businesses to accept payments, knowing that is one of the main form factors for customers walking in the door. It allows them to have the retailer speak for themselves about what they do with the data. It allows them to collect data, and then the speed of the transaction helps reduce times. And then finally, the ability to be online. All it takes is a website and to accept payments is crucial for many small businesses, especially during the pandemic. And we saw all of these technologies play out to help many small businesses continue to thrive during the pandemic.

Mr. DAVIDSON. Yes. Thanks for that. I wish I had time to highlight how many of these technologies that aren't subject to the Durbin Amendment could help small businesses in that way. And Ms. Choudhary, I wish I could have gotten to cold storage. Thanks for referencing it in your written comments.

My time has expired, and I yield back.

Chairman LYNCH. The gentleman yields back.

The Chair now recognizes the gentleman from Wisconsin, Mr. Steil, for 5 minutes.

Mr. STEIL. Thank you very much, Mr. Chairman. Mr. Talbott, my colleagues have attached a bill to today's hearing that they are calling the Protecting Consumers From Payments Scams Act. Scam prevention is a huge priority. In fact, I hosted a scam prevention workshop in my home community of Janesville just last week. But one of my concerns for this bill is that it may not have the desired results. It is looking to have and may have some very significant unintended consequences. Can you talk about how this proposal would impact the electronic transactions ecosystem and the consumers who rely on the services?

Mr. TALBOTT. Yes, sir. Thank you for the question. I think when you think about payments, and these themes have been brought out in the hearing today, there are lots of different payments systems and lots of different use cases for them, and it is important to sort of break them down and understand what they are there for. P2P is largely for sending money between family and friends. It's very different than other forms of payment cards. There are some similarities, but there are differences. So generally, you should think of P2P like cash. It is electronic cash. If you lose money on the sidewalk, it is gone. P2P is not quite the same, but

you should think of it largely as cash, and since it is free, and immediate, and generally irreversible, there is the connection to cash.

Unfortunately, risk is part of our life. Fraudsters are always going to be there. To the extent that we build a 10-foot wall, they are going to build an 11-foot ladder. The key is to build that 12-foot wall, but it is an ongoing thing that we, the payments industry, take very seriously. And the best way to think about focusing on the risks associated with P2P is around consumer education and prompts that have been built into the system. PayPal, for example, has on its webpage a number of disclosures, and Venmo requires a verification of the last four digits of the recipient's phone number for a first-time sale, for example. I think the challenge, though, if you think about the bill, which would expand Reg E, is it might alter the nature of the speed or the cost related to P2P platforms. And that might be an important unintended consequence to consider.

Mr. STEIL. Thank you very much. Let's shift gears a little bit if we can. One of the main focuses of this committee, and of the Select Committee on the Economy, of which I am the ranking member, is financial inclusion. And even though we have made a lot of progress, far too many Americans still don't have access or don't have a bank account or an account with a credit union. And when asked, a significant percentage of unbanked respondents are pointing to two key things, a lack of trust in financial institutions, and inconvenience, as factors that keep them out of the system. How can mobile payments and digital wallets foster greater participation in our formal financial system?

Mr. TALBOTT. That is a great question. Obviously, that is another goal. The major priority for the payments industry is financial inclusion, if I could answer your questions in reverse. In terms of convenience, I think it is obvious the value of the convenience factor that mobile wallets and P2P services provide, just being able to conduct your transactions anytime, anywhere, versus the old days where you have to wait for the bank to open or the credit union to open. Now, you can do it 24/7 at any location.

In terms of accessing a bank account, there are many solutions that exist which allow cash-based taxpayers to access the modern payments world. A simple one is, you can go online. If you want to buy the stocks that the Chair mentioned earlier, you print out a code, you take that code to a retailer, you give them the cash, the retailer scans the code, and the online merchant now knows that the stocks been paid for and releases them to the consumer. So, it is a wonderful way. It is a wonderful technique, technologies that allow cash-based consumers to access the internet and use the payment systems.

Additionally, you can load cash and paper checks directly on to your wallet or your P2P account. Many employers are offering payroll downloaded to your wallet, and none of these require a bank account necessarily. So in terms of convenience and trust, those solutions are working to address that. Lastly, on trust, that is a difficult one that is in the mind of the beholder. I would just say that people don't always trust a bank. They may not always trust the Federal Government, and they may choose not to be part of the system.

Mr. STEIL. I completely agree that they don't trust the Federal Government. I was really concerned that some of my Democratic colleagues put forward proposals to allow the IRS to track inflows and outflows of bank accounts over a certain amount. In a time when we are seeing a large number of people unbanked, we actually go and look at the data, and it says they don't trust banks, financial institutions, and the government. And one of the proposals by my Democratic colleagues is to increase the government's intrusion and review, and breaking the privacy between individuals and their financial institutions moves us in the wrong direction.

I think we have some amazing opportunities with these mobile payments to make sure they are in the hands of every individual, and I would suggest to my colleagues, if we look at some of the Pew Research as to what percentage of folks have access to a smartphone—we dug into that on the other committee—and, in particular, how that travels with age more than it does with race.

With that, I will yield back.

Chairman LYNCH. The gentleman yields back.

The gentleman from Florida, Mr. Lawson, is now recognized for 5 minutes. Welcome.

Mr. LAWSON. Thank you, Mr. Chairman, and Mr. Ranking Member, for having this hearing. I would like to, again, welcome everyone to the committee today.

Mr. Raul Carrillo, funds stored on a wallet are not deposited, and, therefore, are usually not eligible for deposit insurance. Some digital wallets provide something called pass-through insurance, which covers consumer transfer from a direct deposit account to allow it. In this scenario, the Digital Wallet Provider Act acts as a protective agent and deposits the money into the FDIC-insured bank account. Should additional protection be created to ensure that digital wallet users are not under the false impression that their wallets balance are insured? For example, should a wallet provider be required to provide user's disclosure of the details, the type of insurance that covers the transaction, and the difference between that insurance and FDIC insurance? What other protections should we consider to protect users against fraud or loss of funds?

Mr. CARRILLO. Thank you very much for the question, Representative Lawson. I will just first note that I think that this issue speaks to a comment that my co-panelist, Renita Marcellin, highlighted, which is that we often talk about the provision of these wallets as if it supplies somebody with a bank account. However, the very existence and necessity of pass-through insurance indicates otherwise. We have PayPal, et cetera, establishing relationships with banks for the purpose that they aren't providing direct banking services, or they are providing partial banking services but need the rest from a depository institution.

Now, I do not think that pass-through insurance is sufficient to solve this problem. In many cases, what is actually happening is that the wallet provider or a coin issuer is commingling funds and putting those in an FDIC account. This is not a direct relationship between a consumer and a bank, and it does not protect against the failure of the wallet provider or the coin issuer. It just protects against the bank failure, so it is insufficient. Disclosures may or may not be helpful. I think, certainly, we should err in the direc-

tion of providing more notice and disclosure. But ultimately, we have to fix the structural problem here, which is that some wallets are holding funds in long-term custody or custody of any significant duration, and those are not insured. And there is a fundamental problem here in the sense that that should not be allowed, not merely that it shouldn't be disclosed. Thank you.

Mr. LAWSON. Okay. Thank you. And, Ms. McAllister-Young, as more of the country begin to rely on the internet for essential activities, such as banking and financial services, what can be done to ensure that consumers in rural areas, which I represent a lot of, areas which have little to no broadband access, can connect with consumers in heavily-served areas? And what are some other factors that we should keep in mind in terms of community, access to broadband, and the payment system?

Ms. MCALLISTER-YOUNG. Thank you so much for that question. I tend to work with savers and consumers on a day-to-day basis, and access is always top of mind and centered when we think about how we can reach everyone in any corner of America. From our standpoint, at America Saves, it is about education, so also working with people on the ground. We have local campaigns and are working with organizations who have direct interface with people in the rural parts of America, providing them with education, resources, and content that they can disseminate. And there is kind of like a trickledown effect.

As far as the internet and broadband, I am unsure of the answer to that. To be honest with you, that is not really the work that I do. But what I can say is that from the consumer standpoint, it is a huge issue, something that we continue to try to resolve and make sure that we are reaching everyone when it comes to all types of financial education and access to internet and being able to use the mobile wallet.

Chairman LYNCH. The gentleman yields back. I thank the gentleman.

The Chair now recognizes the gentleman from Texas, Mr. Sessions, for 5 minutes. Welcome.

Mr. SESSIONS. Mr. Chairman, thank you very much, and thank you for having this hearing today. I appreciate it very much. I find that our witnesses that we have are up-to-date with it and speaking about a lot of things which I view as interesting, and that is about the education that people bring to the table so that consumers understand what they are getting, what those limitations may be, and they are willing to move forward as they choose.

Ms. McAllister-Young, you spoke clearly about education just a minute ago. Would you mind speaking about if you have knowledge otherwise? And Mr. Talbott, perhaps you might lend some credibility or a hand to it. Talk to me about the education of what might be cryptocurrency users, the kind of people they are, the kind of needs that they have, because I believe, in looking at this for some period of time, that they are highly-educated. They are very smart. They have a fine tune about their dollar, what is theirs, what should be theirs, and how they want to transact, and what they are after, and I find them highly engaged in this process. Could you give me just your overview of ideas, because you were talking about education?

Ms. MCALLISTER-YOUNG. Absolutely. At America Saves, we work primarily with low- to moderate-income earners. And from a perspective of being highly-educated and using cryptocurrency, from my perspective—I can only speak for myself and my peers—everyone, no matter what their income is, has some level of interest in cryptocurrency in their own perspective about if they are ready to jump in the game or not. But because of the work that we do, we are very focused on making sure that prior to jumping into something that could be as risky as cryptocurrency, that they have financial stability in place, meaning they have emergency savings, they know how to save successfully. We say that saving is a habit, not a destination, so building that habit of saving before they jump into something like cryptocurrency.

We also like to say that an informed consumer is an empowered consumer. So. the more information that they can get—unfortunately, even with those who are highly-educated around cryptocurrency, it is changing so quickly and so much that there is always more education to get. And so, the more education and the more informed that we can keep them as things change around cryptocurrency, the better for all. So, while we don't work with a lot of people who are in the cryptocurrency game just yet, our goal is to make sure that regardless of if they are interested in that or not, they have that very foundation of savings first [inaudible].

Mr. SESSIONS. Thank you. That is very thoughtful. Mr. Talbott?

Mr. TALBOTT. Sure. Thank you, Congressman. It is good to see you back.

Mr. SESSIONS. Yes, sir. Thank you. Thank you very much.

Mr. TALBOTT. I think in terms of—

Mr. SESSIONS. Even Chairman Lynch sometimes agrees with that.

Mr. TALBOTT. Looking at the crypto, I think at this point, cryptocurrencies is largely an investment use case which has a different focus: investor protection, and consumer protection. They have not yet moved into the mainstream. We will get there, and stablecoins could serve as a bridge between the investment and the payments use case. But I think your assessment of the investors who are focused on crypto or invest in crypto is correct. I also agree with Ms. McAllister-Young that everybody is talking about this. And that is why the payments industry is spending a lot of time and effort using our current expertise with payments to think about how we incorporate crypto into the broader payment space, so it is more widely available.

There are a lot of questions, a lot of policy issues that have to be discussed and debated. But at this point, it is still on the investment side rather than the payment side.

Mr. SESSIONS. I want to thank both of you for your insight. I will tell you that I enjoy this important task force that is looking at this because I believe that, as the gentlewoman stated here, education is the key to knowledge, understanding, and expectations. And I find, in particular, the blockchain provides a custody similar to what might be back at the old county courthouse, a title that you have to go to. And this is your own title, this is your own authority, this is a thing that you own, and increasingly, as we also develop a discussion today about privacy, knowledge, what is yours, and

even Ranking Member Davidson and Chairman Lynch spoke about the need to understand how you get to your account, and how you keep it, what is your own. And I think that is important.

I want to thank both of you for your thoughtfulness of having this, and, Chairman Lynch, I will do my best to make you love the words. It is good to be back. Thank you.

Chairman LYNCH. Okay. It's good to have you back.

Mr. SESSIONS. Thank you.

Chairman LYNCH. The Chair now recognizes the distinguished gentleman from Illinois, Mr. Foster, who is also the Chair of our Task Force on Artificial Intelligence. You are now recognized for 5 minutes. Welcome.

Mr. FOSTER. Thank you, Mr. Chairman, and I also thank our witnesses. We will just start with a basic question about the concept of ECASH. Is this viewed as similar to cash in that if you lose your device, you are out of luck? If you are subject to fraud, you are out of luck? If someone puts a gun to your head, and drags you into an alley, and says, transfer all of your ECASH to my device, that there is no recourse at that point? It is like they have stolen your cash? Is that the concept, or is there an asterisk on that in anyone's mind?

Chairman LYNCH. Where is the question directed to, Mr. Foster?

Mr. FOSTER. Anyone who is advocating towards the proposal.

Chairman LYNCH. Mr. Carrillo?

Mr. CARRILLO. I am happy to take that question. Thank you, Representative Foster, and thank you, Chairman Lynch. We are trying to replicate the functions of paper cash, and that includes the advantages and disadvantages. In the bill, you will notice that there are error resolution rights or rules around disclosure of error resolution rights similar to EFTA, but those apply to the device rather than to the ECASH itself. So, it is the case that if you lose the device, you are out of luck, and in some instances, this will be unfortunate. However, it is also a mitigating factor against the claims that ECASH will swamp the financial system, and it will cause deposit flight, that it will fundamentally change the nature of what we are doing. We do not expect people to keep their life savings in ECASH, on an ECASH wallet in the same way they don't otherwise.

Mr. FOSTER. Okay. Yes. I understand. So, it will be subject to all the same. Now, is there any concept to prevent it from being used for ransomware?

Mr. CARRILLO. Well, certainly. The use of cash for any illegal activity is illegal, and that is going to exist with us for a while. It is not online, though, and most ransomware involves all of this software that we are talking about, and I would certainly defer to any insight that you, yourself, might have as well.

Mr. FOSTER. So, the ECASH that you envisage cannot be operated online from remote locations? You have to sit there and touch your cards together or something like that?

Mr. CARRILLO. It is not online since it does not use the internet. Now, a different sort of signal can be used, for instance, Bluetooth, the near field communication (NFC) fields that we use for credit card payments, et cetera. On their end, there is a question of at-

tenuation and distance, but, no, it is not for long-distance internet payments.

Mr. FOSTER. Okay. That is interesting. Mr. Talbott, when you start looking at crypto transactions, it seems to me there are two classes then: one, they were just straight payments where you want a dollar in and a dollar out; and two, there is a second class where the crypto may change value. And it seems to me you have to have market regulation. And so, people say how do you prevent wash trades, for example? Say, someone buys an asset from themselves under two different fake names and then establishes a fake market price, sort of a classic abuse to the market. Is there any way to prevent that without having some regulators seeing the true beneficial owner behind every crypto transaction so that they can identify wash trades? Or are there other concepts that might work?

Mr. TALBOTT. Yes. I would have to give that some thought, Congressman, in terms of on the wash. That is more on the investment side rather than on the payment side. But I think your comment about the fluctuation in currencies is one of the hindrances for crypto becoming more mainstream, and a stablecoin could serve to bridge the gap between the two. In terms of wash sales and crypto sales, I would have to look into that and get back to you.

Mr. FOSTER. Yes. It seems to me it is a fundamental problem. Does anyone else have any thoughts on that, that we really have a very separate regulation on identity?

Chairman LYNCH. Ms. Choudhary, would you like to address that?

Ms. CHOUDHARY. Thank you, Mr. Chairman. The identity issue, I would say, has been handled very differently by various jurisdictions, and we do not have a clear answer right now, although some of it is emerging. The European Union has adopted a very different approach for crypto transactions to include information on the parties involved and outlined anonymous crypto transactions for now. But that has obviously raised a concern about how much innovation will come out of the European Union if the same kind of Know Your Customer (KYC) issues are superimposed on that. Major crypto companies have now at least unveiled initiatives that are improving the industry's KYC and anti-money laundering practices. So far, at least, where we have seen cryptocurrencies are involved—

Mr. FOSTER. Yes. Do these innovations allow any single regulator to see the beneficial owner on either side of every crypto transaction, or is that—

Ms. CHOUDHARY. Right now, there is—

Mr. FOSTER. Yes, that seems to be what you have to have here, and I was just wondering if there are identity schemes that actually provide that?

Ms. CHOUDHARY. The digital protocol, which has at least now been introduced by companies like Coinbase and Circle, enables the companies to verify the identities of customers while allowing customers to retain control over their personal information. But in terms of regulators, the regulation right now is not very clear out here other than the travel protocol, which has been laid out.

Mr. FOSTER. Okay. My time is up.

Chairman LYNCH. The gentleman yields back. Thank you very much. The ranking member and I would have liked to go on to another round of questions, but there are votes pending on the Floor, so I am afraid we will have to leave it here.

I would like to thank our witnesses. Thank you so much for your willingness to come here and help the task force and the committee. And thank you for your testimony today.

The Chair notes that some Members may have additional questions for these witnesses, which they may wish to submit in writing. Without objection, the hearing record will remain open for 5 legislative days for Members to submit written questions to these witnesses and to place their responses in the record. Also, without objection, Members will have 5 legislative days to submit extraneous materials to the Chair for inclusion in the record.

This hearing is now adjourned. Thank you

[Whereupon, at 3:55 p.m., the hearing was adjourned.]

A P P E N D I X

April 28, 2022

Testimony before the

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

Regarding

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

April 28, 2022

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

Background & Summary

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

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

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

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

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

---

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

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

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

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

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

Fraud & Error Resolution

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

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

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

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

---

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

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

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

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

Deposit Designation & Banking Regulation

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

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

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

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

---

[6] *See, e.g,* Sarah Jane Hughes & Stephen T. Middlebrook, *Advancing A Framework for Regulating Cryptocurrency Payments Intermediaries*, 32 YALE J. ON REG., 495, 527 (2015).
[7] *See* Dan Awrey & Kristin van Zwieten, *Mapping The Shadow Payment System* 41-44 (SWIFT Institute Working Paper No. 2019-00, 2019), available at: https://ssrn.com/abstract=3462351 (discussing comparative approaches in the U.S., UK, EU, and China).
[8] *See* Dan Awrey, *Bad Money,* 106 Cornell L. Rev. 1 (2020) (discussing how the corporate bankruptcy regime fails depositors).
[9] *See* the STABLE Act, which proposes to regulate stablecoins as bank deposits. Press Release, Tlaib, García and Lynch Introduce Legislation Protecting Consumers from Cryptocurrency-Related Financial Threats (Dec. 2, 2020), https://tlaib.house.gov/media/press-releases/tlaib-garcia-and-lynch-stableact; https://tlaib.house.gov/sites/tlaib.house.gov/files/STABLEAct.pdf
[10] "Ten years ago, tech investor Marc Andreessen famously proclaimed "software is eating the world" … now payments are eating the world." JPMORGAN CHASE, PAYMENTS ARE EATING THE WORLD 4 (2021), https://www.jpmorgan.com/solutions/treasury-payments/payments-are-eating-the-world
[11] President's Working Group on Financial Markets, FDIC, and OCC, Report on Stablecoins (Nov. 2021), https://financialservices.house.gov/uploadedfiles/hhrg-117-ba00-20220208-sd002.pdf
[12] See STABLE Act, *supra* note 9.

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

Data Minimization

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

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

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

---

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

[14] *License to Bank: Examining the Legal Framework Governing Who Can Lend and Process Payments in the Fintech Age, Hearing Before the Task Force on Financial Technology of the Committee on Financial Services*, 116th Cong. (Statement of Raúl Carrillo, Policy Counsel, Demand Progress Ed. Fund & Fellow, Americans for Financial Reform Ed. Fund), https://www.congress.gov/116/meeting/house/111057/witnesses/HHRG-116-BA00-Wstate-CarrilloR-20200929.pdf.

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

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

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

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

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

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

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

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

---

[19] HFSC, Preserving the Right of Consumers to Access Personal Financial Data, 117 th Cong. (Sept. 21, 2021).
[20] Even though they are not new entities, companies like Plaid, Intuit, Finicity, Envestnet|Yodlee, Morningstar/ByAllAccounts, Fiserv/CashEdge, and MX are "barely subject to any regulation, have received little scholarly attention, and most consumers have never even heard of them or know what they do." For timely legal analysis of data aggregators' relationships with banks, tech companies, and consumers in the context of Section 1033, see generally, Nizan Geslevich Packin, *Show Me the (Data About the) Money!*, 2020 Utah L. Rev. 1277 (2020).
[21] Erica Turner, *Americans attitudes and experiences with privacy policies and laws*, Pew Research Center (Nov. 15, 2019), www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/.
[22] Berkeley Media Studies Group et al., The Time is Now: A Framework for comprehensive privacy protection and digital rights in the United States, Citizen.org, (last visited Mar. 31, 2020), https://www.citizen.org/sites/default/files/privacy-and-digital-rights-for-all-framework.pdf
[23] For an extensive list of the most prominent visions of a new regulatory paradigm, see Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics*, 79 Md. L. Rev. 439, 446–47 (2020).
[24] For a general theory of data governance and democracy strongly informing this testimony, *see* Salomé Viljoen, *A Relational Theory of Data Governance*, 131 Yale L.J. 573 (2021).

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

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

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

---

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

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

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

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

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

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

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

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

Separating Commerce & Finance

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

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

---

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

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

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

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

Public Options & Financial Inclusion

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

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

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

---

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

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

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

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

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

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

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

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

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

United States House of Representatives
Committee on Financial Services
The Task Force on Financial Technology
2129 Rayburn House Office Building
Washington D.C. 20515

April 28, 2022
Written Testimony of
Mishi Choudhary

Chairman Stephen Lynch and Ranking Member Warren Davidson and distinguished Members of the Committee, I am pleased to appear before you today on this hybrid hearing entitled, "What's in Your Digital Wallet? A Review of Recent Trends to Mobile Banking and Payment".

My name is Mishi Choudhary and I am the Legal Director of the New York based Software Freedom Law Center that works to protect and advance Free and Open Source Software (FOSS) . Much of the world's most important and most commercially significant software is distributed under copyright licensing terms that give recipients freedom to copy, modify and redistribute the software ("free and open source software"). One could not send or receive e-mail, surf the World Wide Web, perform a Google search or take advantage of many of the other benefits offered by the Internet without free and open source software. FOSS developers create and advance solutions to complex problems that are decentralized, open and accessible to everyone. Several of the world's crypto currencies are built on FOSS and principles of this ecosystem. I would like to note that views presented here are my own.

Money and Digital Technology

In a rapidly evolving technological environment, consumers seek payment methods that are convenient, inexpensive, and secure. Our legacy transaction systems have suffered from high fees, limited access and modest innovation that have beset many financial inclusion efforts. Non-traditional players in the market have attempted to address some of these issues through use of mobile devices to improve access to financial products and services. Digital wallets that use mobile device's wireless capabilities to transmit payment data securely from a mobile device to a point of sale designed to read such data are one such example. Digital wallets may act as either (or both), a storage mechanism for payment details and a storage mechanism for actual funds. In general, they are linked to a bank account, credit, debit or a prepaid card but don't have to. They can hold money and other wallet users can make payment to a user that can be used without involvement of any bank or financial intermediary. These wallets, including but not limited to Apple Pay, Google pay, CashApp, Venmo, Alipay, and others store funds, make transactions and track payment histories. Some of them also store documents like driver's licenses, giftcards, membership cards, hotel reservations inter alia. Mobile solutions that do not rely on bank account access including mobile wallets are particularly attractive to those who don't have access

to a bank account. There are several other peer to peer (P2P) payment services that allow customers to send and receive money electronically between two users that may not fall under the definition of the term wallet. One such popular service is Zelle, operated by Early Warning Services, a company created and owned by seven banks: Bank of America, Capital One, JPMorgan Chase, PNC, Truist, U.S. Bank and Wells Fargo. Some of the features of such apps have also made them a prime target of fraud with little clarity on liability issues, in particular, the application of Regulation E .

Cryptocurrencies are currently stored in hot and cold wallets. Hot wallets come in three forms: Desktop, Mobile and Web and are connected to the Internet, therefore, "hot" in nature. The funds in a hot wallet can be spent at any time, online. Cold storage wallets do not require online servers and can store the assets in the wallets, which are physical devices. Hardware wallets store your cryptographic keys on a piece of hardware that has been specially designed for cryptocurrency transactions. The software program of hardware wallets allows users to keep their assets safe offline and only allows access via private key once the device is connected to the main computer system or device. This adds a security layer reducing the possibility of any cyber-attacks and the absence of a third party ensures that nobody can dictate transactions or access the user's transaction history.

The transition to digital payments was already underway, but the COVID-19 pandemic accelerated adoption to new levels. Despite an uptake in the adoption of these forms of payments, unlike the Chinese or Indian markets that are mobile first, U.S. market still relies heavily on credit cards. A U.S. customer does not necessarily have the same motivation as their Indian or Chinese counterparts especially as credit cards are backed by various laws like the Fair Credit Billing Act, Electronic Funds Transfer Act (EFTA), Credit Card Accountability, Responsibility and Disclosure (CARD) Act amongst others.

We are seeing rapid development and experimentation in cryptocurrencies and various other digital forms of payments, with and without the need of traditional intermediaries. There are growing pains and volatility in these areas but the lessons they offer can help expand the frontiers of digital payment technologies.

Central Banks around the world are considering issuing digital equivalent forms of their currency to the public known as Central Bank Digital Currency (CBDC). Per the Atlantic Council, 87 countries (representing over 90 percent of global GDP) are exploring a CBDC. 14 countries, including China and South Korea, are now in the pilot stage with their CBDCs and preparing a possible full launch. 9 countries have now fully launched a digital currency. [1]

Challenges

As the popularity of these digital payment systems continues to increase, they are increasingly becoming targets of threat actors. In cases, where customers have been targets of fraud, they have not been afforded protections by underlying banks owing to the ambiguity of regulations.

Privacy and Data collection challenges have plagued such wallets. None of the existing offerings can replicate the privacy-respecting features of physical cash. Venmo, owned by PayPal that entered into a settlement with the Federal Trade Commission in 2018 keeps transaction history public by default.

1 Central Bank Digital Currency (CBDC) Tracker, https://www.atlanticcouncil.org/cbdctracker/?params=3f;f;7;f;f&country=&selected= (last visited April 25, 2022)

These can be made private but contact lists remain visible. This feature was what led to the reporters discovering President Biden's account details on the application.

The Chinese example is a cautionary tale with respect to linking of the social credit system and data collection policies where the lines between the Government and private sector are increasingly blurred.

Most of the current solutions cater to the banked customers and don't address those that primarily work in the informal economy or are paid in cash. Such part of the American population also desires the modern conveniences that technology offers without losing the privacy offered by cash.

Opportunities

As we think about money in the age of the Internet, we must design for a future that is in the public's interest, incorporates privacy by design and facilitates financial inclusion. The super apps that are popular in countries like China are gaining popularity around the world, underscore the fact that concerns about data protection and privacy have not been adequately addressed and the current market options lack privacy-oriented messaging system integrated with payments. We need a currency or electronic token that is equivalent in functionality to cash, offers all of its benefits including anonymity, privacy, autonomy, no transaction fee and addresses all of its flaws. Such a design finds support in history as presented by David Chaum[2] in the 1990s and the recently introduced The Electronic Currency and Secure Hardware (ECASH) Act by Rep. Stephen F. Lynch (D-MA) that directs Treasury to commence a two-stage pilot program to test a variety of e-cash technologies and determine the optimum alternative for circulating this electronic currency.

The unique element of the ECASH idea is hardware wallets containing the equivalent of coins created by and managed by the United States Treasury which is as close a way of universal access just like the cash. This idea imagines how everybody can have, store and pay with money without the banking system being involved in any way at all. An idea is to have electronic tokens that are equivalent in functionality to cash and no more traceable. The risk of hard money for working class people has always been loss, inconvenience or inflation. Working people, back to the Jacksonian era in the United States have large experience with ways payment systems chosen by employers have hurt them. So they favor hard money, government coin that is deep in the fabric of democratic finance in the United States, as deep as the importance or role of the elite in the banking system. The questions of identity management like KYC is of great interest to everybody except to ordinary people whose preference is for cash. They live in a world in which informal economy is as important as the formal economy. In the 21st century, it should not matter whether what you are waiving at the cash register is a card issued to you by a bank or a credit union or is a hardware object that United States Treasury has certified, is the way that ECASH is carried around. This structure of ECASH does not have the quality of traceability and preserves privacy. The software underlying any of these technologies must be Free and Open Source to enable public review and audit of the source code for potential security issues.

If used correctly with adequate guardrails, digital money presents an opportunity for financial inclusion for those with little access to formal banking systems. Any such efforts must provide consumer protection and data privacy, aspects often found to be woefully lacking in several such offerings around

2 David Chaum, *Achieving Electronic Privacy*, August 1992, https://www.chaum.com/publications/ScientificAmerican-AEP.pdf

the globe. What we need is to have more multi-disciplinary research in development of technologies that work for those that are most disadvantaged by the current system, those who don't have bank accounts and have to pay high fees to access their cash built with privacy by design.

Thank you for the opportunity to appear before you today, and I look forward to your questions.

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)

Testimony of Kia McCallister-Young, Director of America Saves

before the Task Force on Financial Technology, U.S. House Committee on Financial Services on

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

April 27, 2022

Chair Lynch, Ranking Member Davidson and members of the Task Force, it is an honor to be invited to testify and contribute toward the on-going conversation of digital wallets and mobile payments. My name is Kia McCallister-Young and I am the Director of America Saves, a national campaign that focuses on building financial stability, resilience, and confidence, particularly with low to moderate income earners — supporting them in their quest to save successfully, reduce debt, and get on a path toward building wealth. America Saves is an initiative of the Consumer Federation of America (CFA), a non-profit association of approximately 250 pro-consumer groups that was founded in 1968 to advance the consumer interest through research, advocacy and education.

While there are many areas of concern regarding mobile banking including, peer to peer payments, financial technology loan and credit products; my specific testimony will highlight the consumer voice and experience as related to mobile banking and payments,while working toward policy and regulation.

Experts agree, including advocates at CFA, that concerns about this topic include the high prevalence of fraud and scams, a lack of accountability and oversight, minimum consumer protections beyond disclosures and warnings, ineffective consumer privacy as it pertains to financial data, and an overall need to strengthen federal and state oversight to name a few. My work at America Saves allows me to interface and engage on a continual basis with everyday consumers, many of whom are oblivious to the risks undertaken when using digital payment options, as opposed to cash, credit, or debit cards.
Their choice to use said platforms is largely due to the convenience factor coupled with the lack of transparency of risks, purposefully orchestrated by the platforms. Consumers naturally trust these payment options because a clear delineation between banks, credit unions, and mobile payment applications does not exist. The result of that opaqueness is the belief by consumers

that mobile payment options are regulated with the same level of scrutiny as other financial institutions.

This incorrect belief results in misguided trust among consumers, leaving them vulnerable to aforementioned risks like fraud, scams, and payments being held by the platforms with very limited and, at times, no recourse at all. These products can play a role in helping consumers manage their finances, but federal and state oversight is needed to ensure consumers are protected from harmful practices, fraud, scams, and violations of data privacy.

This occured to me in 2018 when PayPal held funds of my own that were paid through a third party processing company. It was unclear for several days who I was to reach out to for resolution. Paypal said it was the third party processor, the third party processor said it was my bank, and my bank said it was PayPal. Meanwhile, I was unable to pay for basic needs for my family while it got sorted. It took over 30 days for my funds to become available to me.

The lack of clarity, consumer protections, and transparency is not evident to consumers until it's too late.

Usage of fintech products has dramatically increased despite lack of sufficient regulation and oversight. The Covid-19 pandemic and the heightened sensitivities to health, public touching, and not seeing loved ones only added to the uptake of mobile payments, leaving Americans feeling it is the only (quick, available) option for payments. In addition, inflation is driving the low-to-moderate income earners toward fintech credit products and the need to access their pay early. Furthermore, without more oversight, immigrant citizens who often send money back to their families in their native countries remain disproportionately subject to alarmingly high remittance fees.

Because the foundational motivations for use of mobile payment applications are likely not to change, the onus to protect consumers through education, transparency, policy, oversight, and regulation simply must be prioritized. As we work to rebuild our economy and increase financial resilience for every American, we must recognize and highlight what threatens our nation's ability to save, reduce their debt, and build wealth. That work is an intersectional joint effort of financial education through content, resources, and support along with policies and regulation that protect consumers from practices that make it hard for consumers to be fully informed through complexity and suppression of information and easy, clear access and warnings of risk.

I thank you for your time and the opportunity. Please reach out with questions and comments to kyoung@consumerfed.org.

America Saves is an initiative managed by the nonprofit Consumer Federation of America that uses the principles of behavioral economics and social marketing to motivate, encourage, and support low- to moderate-income households to save money, reduce debt, and build wealth.

The Consumer Federation of America is an association of more than 250 nonprofit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education.

ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

Testimony of Scott Talbott, Senior Vice President of Government Affairs of ETA

Before the House Task Force on Financial Technology Hearing on

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

Chairman Lynch, Ranking Member Davidson, and members of the Task Force on Financial Technology, my name is Scott Talbott and it is my privilege as Senior Vice President of Government Affairs of the Electronic Transactions Association (ETA) to submit this statement on how digital wallets and similar innovative payments technologies are providing consumers and small businesses with safe and convenient tools for buying goods and service and transferring funds from person-to-person (P2P).

In addition to powering our economy, digital wallets play an important role in promoting inclusive banking and financial services, and they proved an invaluable tool for distributing economic stimulus payments during the COVID-19 pandemic. On behalf of ETA and its members, thank you for the opportunity to participate in this important discussion, and I look forward to discussing these exciting developments with the Task Force today.

I. Background on ETA and the Payments Industry

Before jumping into digital wallets in detail, it might be helpful to introduce ETA and explain the role of our members in powering the economy.

ETA is the leading trade association for the electronic payments industry, representing over 500 companies that offer electronic transaction processing products and services, including credit and debit card processing, P2P products, digital wallets, and other forms of digital payments. ETA's members include: financial institutions; payment processors; payment facilitators; mobile payment service providers; digital wallet providers; software service providers; companies providing security services; and non-bank online lenders that make commercial loans to small businesses, either directly or in partnership with other lenders.

Each year, ETA member companies spend billions of dollars on research to develop and deploy new products and services that securely move trillions of dollars in payments. To put the electronic payments industry in context, during 2020, consumers and businesses spent $7.84 trillion in card volume in the U.S.[1] and another $1 trillion was moved over the largest P2P networks — many of these transactions facilitated seamlessly through digital wallets. Combined, these equate to 40% of the U.S. GDP in 2018. During 2019, ETA members helped global consumers and businesses make $24.3 trillion in purchases; that number is expected to grow to $24.6 trillion in 2023.[2] The infrastructure supporting this system is sophisticated,

[1] https://www.federalreserve.gov/paymentsystems/december-2021-findings-from-the-federal-reserve-payments-study.htm
[2] https://www.statista.com/

ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

secure, and fast — processing over 300,000 transactions per minute. The electronic payments system is also reliable — it operates 24/7/365, in the U.S. and around the globe, without interruption. And ETA members are not slowing down; the industry is constantly investing and innovating, creating new financial services and payments products that benefit individuals and small businesses alike.

Thanks to our industry, individuals and merchants have a wide array of electronic payment options available that allow them to instantly and safely transfer money to one another, store their money and their credit cards on their smartphones, buy products and services online, and quickly and safely purchase goods in stores with the mere tap of a card or phone. That innovation has accelerated in recent years in response to consumer demand and has been fueled by competing technologies, such as the development of digital wallets

II. Overview of Digital and Mobile Wallets

Every day, Americans use digital wallets to pay for coffee on the way to work, make secure payments at stores, and pay babysitters when taking time out with friends and family. But what is this technology, and how does it work?

Digital wallets can be defined broadly to include mobile and other online applications that allow users to process payments, access account information, and pay for services. Digital wallets provide users with access to stored payment credentials, which may include a credit or debit card, bank account, or, less commonly, a prepaid or gift card linked to the phone or app. This technology has gained popularity with consumers as a safe and convenient way to transmit funds in multiple settings, including for online purchases, payments at brick-and-mortar retailers, and person-to-business (i.e., bill pay) and P2P transfers. The concept of the digital wallet has been swiftly embraced by the public due to its ease of use. The user just has to download and register a mobile wallet app on his or her phone.

The benefits of digital wallets are numerous. By leveraging existing payment technologies, such as credit cards, automated clearing house (ACH) payments, or bank accounts, digital wallets allow consumers to make payments at almost any store in the country. Moreover, wallets are almost always accessible through a consumer's phone or online, which makes them easy to use in person or through a computer or tablet and enhances merchants' ability to meet consumers where they are – literally (aka omnichannel). In most cases, the transfer of payment is free for the user and comes directly out of his or her bank account or credit card (which they have linked to the mobile application). Put differently, consumers and businesses have safe and convenient payments right at their fingertips, whether for purposes of buying goods or services or for sending money to friends and family.

Digital wallets are not only ubiquitous, but they are also highly secure. The industry employs a multi-level approach to security. To access a smartphone, some form of authentication is required such as biometric (fingerprint, face recognition) or entry of a pin. The use of new authentication methods to verify and authenticate transactions helps minimize potentially fraudulent transactions. These new tools include the use of the following: tokenization, biometric authentication, including the use of thumbprints, facial, and voice recognition; and geolocation that compares the merchant's location with the location of the

ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

consumer's phone. Visa estimates that AI analytics helped reduce payment card fraud by $26 billion in 2021.[3]

Additionally, the payments industry has introduced point-to-point encryption (P2PE) and the tokenization of data to minimize or eliminate the exposure of unencrypted data in connection with a purchase. In most cases, digital wallets do not hold any actual payment card numbers, instead converting the payment card number to a token. When making a transaction, it is the token that is transmitted to the issuing bank, which converts the token back to the account number. Thus, even if a transaction using a mobile wallet was compromised, the bad actor would only have access to a token that could not be used to commit fraud. Visa estimates that tokenization has led to a 2.5% increase in approval rates for merchants and has reduced fraud by 28%[4].

In addition to security, another important feature of digital wallets is that they are contactless, which means that they allow a consumer to make a purchase by simply tapping the card or device at a terminal. Contactless products often use a technology called Near Field Communication (NFC), which allows the card or phone to communicate with the terminal when cardholders place their payment card or mobile phone near it.

Consumers are increasingly adopting contactless payment because it allows them to pay without touching anything other than their own card or their own phone. They are not required to hand their card to a cashier or dip or swipe their card into the point-of-sale terminal. The use of contactless payment methods proved invaluable during the pandemic. For example:

- According to a Fiserv study, nearly 24% of respondents believed mobile payments were the safest to prevent the spread of the virus, compared to 6% of respondents saying cash was safest and 4% saying checks were. Nearly 67% of mobile payment users expect the increased use to be permanent.[5]

- A Mastercard Global Consumer study (April 2020) found that between February and March 2020, contactless transactions grew twice as fast as non-contactless transactions in grocery and drug stores.[6]

- Visa[7] reported that in March 2020, 31 million Americans tapped a card or mobile device, a rate that is almost 50% higher than it was six months prior; and from March 2019 to March 2020, there was a 150% increase in contactless payments.

---

[3] https://usa.visa.com/dam/VCOM/blogs/visa-trust-in-digital-payments-infographic.pdf
[4] https://usa.visa.com/dam/VCOM/blogs/visa-trust-in-digital-payments-infographic.pdf
[5] https://www.fiserv.com/en/about-fiserv/resource-center/consumer-research/2020-expectations-experiences-consumer-finances-covid19.html?_ga=2.206902867.1552485462.1615948799-1459718161.1615948799
[6] https://www.mastercard.com/news/press/press-releases/2020/april/mastercard-study-shows-consumers-globally-make-the-move-to-contactless-payments-for-everyday-purchases-seeking-touch-free-payment-experiences/
[7] https://usa.visa.com/visa-everywhere/blog/bdp/2020/04/30/merchants-and-consumers-1588276426783.html

ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

- Nearly one-third of the US population uses NFC to make payments at POS locations.

- Based on data from PaymentsSource's Future of Money Survey released in November 2020, 48% of Gen Z survey respondents stated that they would be extremely or very interested in using a mobile wallet as a primary payment method for all in-store transactions. Millennials scored even higher, at a 61% level.[8]

- Gen Z went from 3% mobile wallet usage as a primary payment method in February 2020 to 9% in November 2020, and millennials went from 2% to 7% in the same time period. Consumers above the age of 75 are also adopting mobile wallet payments. Although seniors' use of digital wallets remains around 7%, it experienced a three-fold increase from 2% in 2019.

Put simply, digital wallets have grown dramatically in popularity because they provide consumers and businesses with safe and convenient payment options.

On this point, I'd like to take a brief moment to recognize the important role that the payments industry — including digital wallet providers — played in helping consumers and businesses weather the many challenges of the COVID-19 pandemic. It is worth noting that during the heart of the pandemic, over 4 million payments were distributed via prepaid debit cards and the providers were able to keep the fraud to a record low percentage.

ETA's members helped the federal government deliver billions in stimulus money under the CARES Act, especially to low-income Americans, including Economic Impact Payments and unemployment benefits. Over four million payments were distributed by prepaid debit cards, with many of these cards capable of being stored safely and conveniently in digital wallets for future use.

In addition, with COVID-19 having forced most of the country to shelter in place for weeks at a time, digital wallets provided a way for consumers and businesses to engage in necessary transactions, such as paying remotely for the delivery of groceries, paying restaurants for curbside or delivery services, and transmitting funds to family members. As discussed, digital wallets, in particular, helped support social distancing by offering a "contactless" way for consumers to pay for goods and services without touching public equipment or passing cards back and forth to cashiers. All of the benefits combined to make digital wallets a critical tool during a time of great uncertainty in our country.

III. Digital Wallets Are Subject to a Comprehensive Legal Framework

While it is clear that digital wallets offer consumers and businesses numerous benefits, it's equally important to recognize that these services are offered within a robust federal and state legal framework. ETA has published a white paper on the *Overview of Laws and Regulations Governing Payments and*

[8] https://arizent.brightspotcdn.com/e0/4f/07e37f224befa7a43e60383471d2/future-of-money-report-final-2020.pdf

ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

Related Services[9] that provides a detailed outline of relevant federal and state laws. A few such laws are worth highlighting. Mobile wallets, depending on how they are structured, may implicate the Bank Secrecy Act and state money transmission laws, the Electronic Fund Transfer Act, information security requirements, the Gramm-Leach-Bliley Act, the CFPB's prepaid account rule, federal and state prohibitions on unfair and deceptive acts and practices, among many others. In addition, digital wallets are often provided through relationships with banks and other regulated financial services providers, meaning that wallet providers are generally required by contract to comply with various legal and regulatory obligations pushed down by the bank or financial services partner.

And that is just the beginning. The payments industry has always been a leader in self-regulatory efforts, including the development of robust and sophisticated self-regulatory programs to further protect the integrity of the payments ecosystem and the consumers and businesses that rely on it with every transaction. These self-regulatory programs govern many of the payment methods offered through digital wallets, including credit and debit cards and ACH transactions.

The card brand rules also establish customer due diligence, contract, transaction monitoring, and data security requirements. In particular, the payments industry took the lead in developing the Payment Card Industry Data Security Standard (PCI-DSS) for handling the safety of cardholder data. The PCI-DSS sets forth requirements designed to ensure that companies that process, store, or transmit credit card information maintain a secure environment for such data.

Finally, the payments industry has a long history of fighting fraud through robust underwriting and monitoring policies and procedures. With the benefit of decades of expertise, ETA members have developed effective due diligence programs to prevent fraudulent actors from accessing payment systems, monitor the use of those systems, and terminate access for network participants that engage in fraud. Working with its members and industry and government stakeholders, ETA has published various guidelines that provide underwriting and diligence best practices for merchant and risk underwriting, including the "Guidelines on Merchant and ISO Underwriting and Risk Monitoring" and "Payment Facilitator Guidelines."

These are just some of the tools that the payments industry has developed in recent years to fight fraud, protect consumers, and ensure the integrity of the payments ecosystem. These efforts have been remarkably successful in reducing fraud while ensuring that consumers have access to fast, reliable, and safe payment options.

IV. Digital Wallets Support Financial Inclusion and Access to Financial Services

Finally, I'd like to emphasize the payments industry's commitment to financial inclusion, and the important role that digital wallets play in providing all Americans with access to safe, affordable, and convenient payment options.

---

[9] https://www.electran.org/wp-content/uploads/ETA-WP-FedStatePayments-1.pdf

ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

ETA member companies continue to advance the global flow of commerce while delivering affordable financial tools and services that meet the needs of underserved consumers. Financial inclusion needs remain significant and urgent, however, a goal of ETA member companies is to continually enhance the electronic payments and financial ecosystem so that it is accessible to all consumers, while ensuring that their transactions can be completed securely, efficiently, and ubiquitously. A key driver to achieving such a system is the development of new technologies such as digital wallets, which have proved invaluable in helping the traditionally underserved consumers access financial products and services. In the U.S., 98% of the adult population has a mobile phone and of those, 81% are smartphones, a steady increase from previous years. Utilizing a mobile device as a primary method of account access enables greater financial literacy by allowing consumers to manage their accounts from their fingertips.

Expanding the ability to access the financial system not only empowers consumers to take control of their financial well-being but also creates a more resilient and inclusive economy. See ETA's annual white paper on *How Fintech Is Addressing the Financial Needs of the Underserved*[10].

By leveraging mobile and other online systems, digital wallets provide consumers with access to safe and convenient financial services. This allows underserved consumers, in particular, to move away from cash-based transactions and gain access to more traditional financial services. In addition, the facilitating of P2P transactions helps underserved consumers move money more efficiently within a safe and secure environment. These are just a few of the reasons why digital wallets have proved so popular, particularly with younger generations that have less experience with traditional financial services.

V. Conclusion

The payments industry is innovative, dynamic, and competitive, focused on delivering cutting- edge products with robust security measures to help consumers connect with merchants, make payments, and move money. Digital wallets are a great example of this innovation. They provide all Americans with access to safe, affordable, and convenient payment methods that can be used in stores, online, and to make P2P payments. And while digital wallets are a remarkable development, the modern payments industry is already hard at work developing the next generation of products, services, and fraud prevention technologies to help individuals move money.

[10] https://www.electran.org/wp-content/uploads/ETA-Creating-a-More-Inclusive-Economy-2022-2.pdf

Statement for the Record

On behalf of the

American Bankers Association

before the

Task Force on Financial Technology

Of the

House Financial Services Committee

April 28, 2022

Statement for the Record

On behalf of the

American Bankers Association

before the

Task Force on Financial Technology

House Financial Services Committee

April 28, 2022

The American Bankers Association[1] (ABA) appreciates the opportunity to submit a statement for the record for the hearing titled "What's in Your Digital Wallet? A Review of Recent Trends in Mobile Banking and Payments."

Today, the U.S. dollar is largely digital. American companies lead the world in creating the technologies that underpin digital payments, but there are risks to our continued leadership. It is important that Congress remain vigilant and deliberate in its policymaking to ensure that our regulatory environment supports innovation rather than overregulating or replacing private sector innovators. From damaging card "routing"[2] requirements currently proposed by the Federal Reserve Board in a redesigned Regulation II to failing to ensure consistent consumer protections and data security standards, bad policy can undermine the potential for a fairer, more efficient payment system.

Innovation Pays: America's Payment System is Working

Americans are rapidly embracing new payments technology that meets them where and how they live. Smartphones, voice assistants, and wearables have brought financial services from the teller line and desktop computer to the pockets and wrists of consumers. New small businesses have come into being because of mobile phone-based card acceptance solutions and many retailers were able to stay in business

[1] The American Bankers Association is the voice of the nation's $23.7 trillion banking industry, which is composed of small, regional and large banks that together employ more than 2 million people, safeguard $19.7 trillion in deposits and extend $11.2 trillion in loans. Our members, located in each of the fifty states and the District of Columbia, include banks, savings associations, and non-depository trust companies of all sizes. ABA works on behalf of nearly all of the more than twelve hundred FDIC-insured institutions that provide trust and fiduciary services to individual and institutional customers.

[2] ABA, credit union organizations, minority banking representatives, and over 1,000 community financial institutions are calling on the Federal Reserve Board to withdraw its incomplete and arbitrary 2021 Notice of Proposed Rulemaking (Regulation II) to administratively expand the Durbin Amendment beyond the scope anticipated or intended by Congress. This Proposal, which does not comply with administrative law and is implausibly called a 'clarification,' would place community financial institutions at a disadvantage, encourage more fraud, and raise the overall cost of payments. We vigorously oppose adopting this Proposal, unless it is significantly revised and reproposed.

during the pandemic because the payments industry came into the crisis prepared with flexible options. Contactless payments are speeding up turnstiles on the nation's transit, including Washington's Metro and New York's subways.[3, 4] From government benefit cards accepted anywhere to remote check deposits, banks are making payments more inclusive. Increasingly, transactions happen within apps and online, without any physical payment credential being tendered.[5]

In a recent Morning Consult poll, 97% of adults rated their banks' online and mobile app experience as "good" to "excellent." Further, 81% reported that recent tech improvements delivered by their bank are making it easier to access financial services. [6] This month, a report[7] from a merchant technology provider found that 84% of business locations accept contactless payments and 9% of consumers describe digital wallets as their preferred form of payment, with contactless cards at 36%. Nearly three-quarters of consumers say that contactless payment types are convenient and easy to learn.

The U.S. Dollar is Digital

The vast majority of money in the United States is electronic and created by private banks. Though the exact percentages are not known, a study of a similar economy found that **97% of money in use was digital money created by commercial banking** whereas 3% was cash from the central bank.[8] There is not a need to end the issuance of cash, nor is there a looming technological challenge that urgently requires us to convert paper money into public digital currency. Simply put, digital money and paper money do not compete and the continued existence of paper money does not present evidence of our government falling behind. Cash has its own benefits, many of which do not survive when attempts are made to create a digital version of it, and we argue that the distinction between central bank money and electronic bank money should be preserved so that the unique benefits of each be conserved. There has been much made of the need for the central bank to issue a "digital dollar," but once the expensive architecture required is fully explored, the end state for consumers is not much different than what we have today. This realization may be why several central banks have abandoned movement towards a Central Bank Digital Currency (CBDC)[9]. At this time, we do not see the case for a CBDC in the U.S.

Will Tomorrow's Payments Be a Step Forward or Backwards?

New payments options are being broadly adopted in our society. But this revolution is underpinned by technology which, while ubiquitous, may not be available in the same way to all consumers. Questions of equity and access have rightfully been raised for answer by the technology sector, merchants, and financial services companies. The best way to provide access to mobile payments is through a bank account and

---

[3] SmarTrip on iPhone & Apple Watch. WMATA. https://www.wmata.com/fares/MobilePay/ApplePay.cfm

[4] Say Hello to Tap and Go, with OMNY. NYC MTA. https://new.mta.info/system_modernization/omny

[5] *The Changing Face of the Payments System: A Policymaker's Guide to Important Issues*. American Bankers Association, 2013. https://www.aba.com/news-research/references-guides/changing-face-payments-system

[6] Morning Consult poll of 2,201 U.S. Adults, Sponsored by ABA. Oct. 1-3, 2021.

[7] *Emerging Trends at Point of Sale*. Hanover Research. 2020.

[8] Mcleay, Radia, and Thomas. *Money Creation in the Modern Economy*. Bank of England, 2014.

[9] *Central Bank Digital Currencies: Policy Issues.* Congressional Research Service, 2022. https://sgp.fas.org/crs/misc/R46850.pdf

ABA's members offer digital-first, affordable options, including Bank On-certified accounts. The Economic Impact Payments (EIP) disbursements leveraged electronic channels, including bank-powered prepaid cards[10] and Direct Deposit, to put money in the hands of people faster and we should strive to further develop the government's use of available private sector conduits to deliver funds without resorting to paper checks that can take weeks to print and to mail. The more efficient and secure provision of government disbursements to citizens is one of the main promises of digital payments that lay in the control of the Congress and the Administration. Our industry stands ready to support these improvements and we urge a whole-of-government focus on better serving recipients and protecting federal funds from fraud or loss.

Mobile and Digital Channels Should Bring High-Quality Banking Services to More Americans

The increasing use of mobile payments can be a force for good, however we should guard against regulatory loopholes that leave Americans with lower quality payments experiences. True innovations deliver the same or better service in new ways rather than by lowering existing standards. Fair and level regulatory playing fields protect consumers, support the stability of the financial system, and mitigate moral hazard that may occur from a race to the bottom. We are concerned by indications that the Federal Reserve may be considering whether to grant entities that have no federal supervision and deposit insurance direct access to its core interbank payment settlement systems.[11] We urge Congress to enact legislation to prohibit such arrangements.

Educating Consumers and Tackling Fraud are Essential

During a prior task force hearing, a consumer group witness rightly stated that "mobile is a platform, not a payment type" and noted that consumer protections for mobile transactions are tied to the underlying payment type. One of the challenges that must be acknowledged is that some new payment products function differently from other well-established payment channels.

Digital transactions tied to payment types like credit and debit cards carry strong protections, in large part due to network rules that require due diligence on who is allowed to accept network payments. Consumers are now using newer payment types that allow them to pay not just vetted merchants but friends, families, and others who have a bank account. To ensure broad access to bank accounts, the criteria for opening a bank account is not as strict as the criteria for accepting card network payments. Thus, these new payment types require a different understanding of risk of loss and the ability to identify fraudulent transactions before they are sent and to recover funds after they are sent. Fraudsters see peer-to-peer payments as a new, additional payment channel and are exploiting this transition and education phase using social engineering on platforms outside the payment system that they then monetize through the peer-to-peer payment channel. While banks are constantly evolving their interfaces to combat fraud that is within their ability to control, the misuse of peer-to-peer and crypto payment systems is, admittedly, an area that requires consistent action by industry.

---

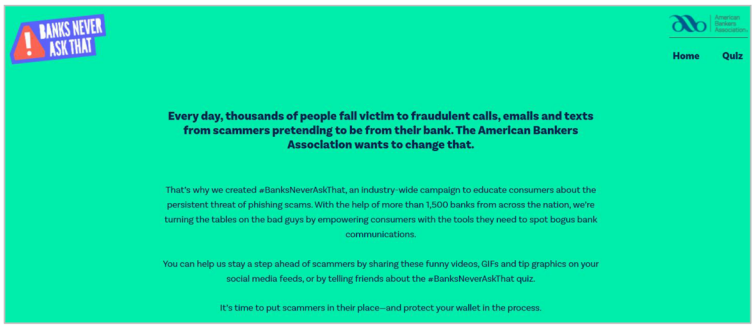
[10] Economic Impact Payment (EIP), Prepaid Debit Cards. Consumer Financial Protection Bureau. https://www.consumerfinance.gov/coronavirus/managing-your-finances/economic-impact-payment-prepaid-debit-cards/

[11] *Re: Guidelines for Evaluating Account and Services Requests*. BPI, 2022. https://bpi.com/wp-content/uploads/2022/04/BPI-Joint-Trades-Comment-Letter-to-Federal-Reserve-re-Fed-Accounts-Supplemental-Proposal-2022.04.21.pdf

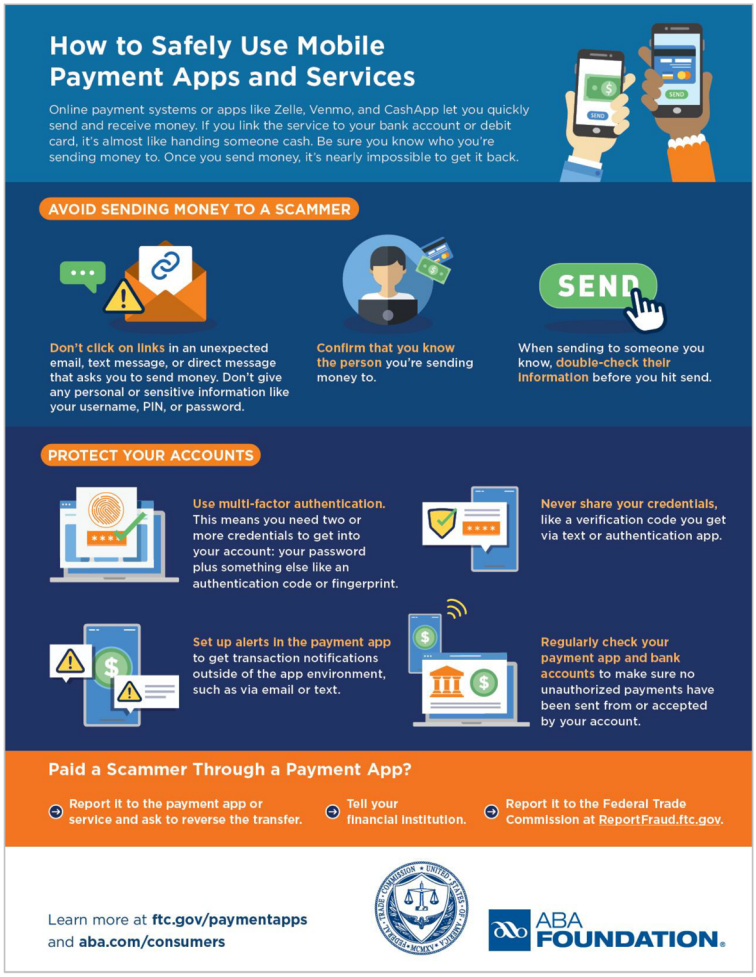
At the same time, if peer-to-peer payments are to continue to exist, there should be a pragmatic delineation between *payments fraud* and the myriad types of fraud that might be incidentally facilitated through the peer-to-peer payment systems — which are simply another channel to make payments, and thus will be a target for fraudsters. For example, cash is so commonly used for fraudulent purposes that possessing large amounts of it is a potential marker of wrongdoing and the government takes the balanced approach of regulating certain cash transactions. Yet, the U.S. Treasury does not reimburse consumers if they unknowingly buy a counterfeit item with cash, even though the government's payment system facilitated the transaction. Despite this fact, some still suggest that banks should reimburse consumers for any peer-to-peer transactions that may be associated with fraud, regardless of the circumstances. An overreliance on regulation of payment media is unlikely to reduce overall consumer losses and will merely redistribute them in a different way.

Banks have a strong and clear interest in preventing fraud and protecting their customers. Consumer education coupled with industry efforts to prevent fraud are key. According to a 2020 ABA survey, banks are estimated to prevent about $22 billion a year in attempted fraud.[12] ABA's members are on the front lines of educating consumers about the safe use of payments apps. Most recently, ABA has partnered with the Federal Trade Commission (FTC) in promoting educational materials about payment app scams (see April 2022 infographic on following page). In addition, ABA has launched a consumer education campaign that activates banks and their customers about the social engineering tactics of scammers. Called "Banks Never Ask That!," the campaign includes interactive and social elements to help customers stay ahead of these scams. We also applaud the educational work of the Consumer Financial Protection Bureau (CFPB) and state officials.

We greatly respect the views of consumers groups who (like our members) are working to analyze these complex issues. We welcome dialogue with the Task Force on this point.



[12] *Banks Prevented More Than $22B in Fraud Attempts in 2018.* ABA Banking Journal, 2020 https://bankingjournal.aba.com/2020/01/aba-report-banks-prevented-more-than-22b-in-fraud-attempts-in-2018/


How to Safely Use Mobile Payment Apps and Services
Online payment systems or apps like Zelle, Venmo, and CashApp let you quickly send and receive money. If you link the service to your bank account or debit card, it's almost like handing someone cash. Be sure you know who you're sending money to. Once you send money, it's nearly impossible to get it back.
AVOID SENDING MONEY TO A SCAMMER
Don't click on links in an unexpected email, text message, or direct message that asks you to send money. Don't give any personal or sensitive information like your username, PIN, or password.
Confirm that you know the person you're sending money to.
SEND
When sending to someone you know, double-check their information before you hit send.
PROTECT YOUR ACCOUNTS
Use multi-factor authentication. This means you need two or more credentials to get into your account: your password plus something else like an authentication code or fingerprint.
Never share your credentials, like a verification code you get via text or authentication app.
Set up alerts in the payment app to get transaction notifications outside of the app environment, such as via email or text.
Regularly check your payment app and bank accounts to make sure no unauthorized payments have been sent from or accepted by your account.
Paid a Scammer Through a Payment App?
Report it to the payment app or service and ask to reverse the transfer.
Tell your financial institution.
Report it to the Federal Trade Commission at ReportFraud.ftc.gov.
Learn more at ftc.gov/paymentapps and aba.com/consumers
ABA FOUNDATION.

Private Sector Innovations Shouldn't Be Stifled By Premature Regulation

The mobile wallet marketplace has rapidly scaled up through the collaboration of regulated financial institutions and technology companies, including many startups. This evolution is far from over, likely not even through its first phase. Consumers and merchants have a wide variety of options and the architecture of mobile payments is certain to change as lessons are learned and competition plays out. Proposals to short-circuit this growth by picking "winning" models would be a mistake.

Regardless of the Future of Cash, More Access to Electronic Payments is Key

More than virtually any sector, banks are in the cash business – it is merchants, however, who decide which forms of payment they will accept. Cashless policies matter most when there is not adequate access to electronic payments – one strategy to mitigate underlying cash policy concerns is to work together to grow banking options for the underbanked. In the age of in-app payments, it is possible that access to electronic payment tools like debit cards and payment apps may become as important as basic internet access was at the height of the "digital divide." Unfortunately, access to basic banking accounts and debit cards has been reduced by the archaic and obsolete Durbin Amendment, pushing some consumers to inferior financial services options that are not readily loadable into mobile payment apps. Repealing the Durbin Amendment would allow more people to qualify for free or low-cost, high-quality deposit accounts that support mobile payments. This increased access would reduce the impact of cashless policies chosen by merchants.

Paying with a Bank is Rewarding

Studies consistently show that card rewards programs are extremely popular[13, 14] – America's banks are proud to provide ways to pay that turn into holiday trips, cash back, and other benefits for American families.

While some media commentators have claimed that rewards cards create a "Reverse Robin Hood" effect, they fundamentally misstate the economics of payments and loyalty/rewards programs. In fact, rewards cards are among the most progressive of financial products, and are widely held across risk tiers and card types while providing the consumer with what is effectively a discount versus cash payments or non-rewards electronic payments. Using data from 2020, the Consumer Financial Protection Bureau (CFPB) found that over 60% of subprime credit cards and 70% of near-subprime cards featured rewards. For average risk borrowers (prime tier), 80% of credit cards feature rewards.[15] Since consumers often own both rewards and non-rewards cards, it is likely that these statistics underestimated *people* using rewards.

Last year, an ABA white paper summarized the benefits to consumers and merchants alike, including lower-income consumers, of credit card rewards.[16] Among other findings, the paper concluded households of all incomes benefit from rewards cards, that most interest is paid by higher-income cardholders, and that

---

[13] *Emerging Trends at Point of Sale*. Hanover Research, 2020.

[14] *The Value of Rewards*. Electronic Payments Coalition, 2019. http://www.electronicpaymentscoalition.org/wp-content/uploads/2019/03/EPC-Value-Of-Rewards.pdf

[15] *Report on the Consumer Credit Card Market*. Consumer Financial Protection Bureau. 2021

[16] *The Benefits of Credit Card Rewards: How Rewards Provide Value to Merchants and Consumers of All Incomes*. American Bankers Association, 2021. https://www.aba.com/news-research/research-analysis/the-benefits-of-credit-card-rewards

credit card rewards are not a wealth transfer. The paper also found that merchants gain far more from credit card rewards programs than they pay in transaction fees. These benefits accrue through higher purchase values, increased security, lower risks, and avoided costs of cash. Moreover, there is little evidence that merchants pass the costs of card acceptance through to consumers — which is intuitive, given that the benefits of card acceptance outweigh the costs — so lower-income cash and debit users do not subsidize rewards through higher prices.[17]

Some back-of-the-envelope analyses that are critical of credit card rewards use overly-simplified scenarios to model earning and spending habits, with assumptions often at odds with available data on consumer behavior and real reported satisfaction with actual card products.

The reality is that while there is a Reverse Robin Hood effect in the rewards payments marketplace, it is one created by regulation and not banks: the loss of rewards on *debit* cards due to the Durbin Amendment has allowed some large merchants to increase profits. For checking accounts covered by Durbin, the minimum balance required to avoid fees increased 50% after the law came into effect.[18] During the same time period, large merchants received over $50 billion in benefits from the law.[19] Many bank customers can now only access rewards programs if they can qualify for a credit card. This is the definition of Reverse Robin Hood – using the force of law to remove benefits from basic financial products such as debit cards in order to increase profits at large global retailers. Many of the current discussions about the "real value" of rewards are really arguments about the costs to merchants of payment acceptance.

Simply put, electronic payments are ubiquitous, competitive, and advancing faster in the United States than anywhere else in the world. Our innovators produce payments tech adopted the world over.

The Cashless Question

Banks offer their merchant partners a wide range of payment choices. These include, primarily, cash handling and electronic payment services such as payment card acceptance. The choice to accept or not accept a form of payment is one made by merchants, often through consultation with a third-party technology provider that may offer "payment optimization" services. Banks do not press merchants to eliminate cash, and in fact, banks continue to support the nation's cash infrastructure through ATM sponsorship, night cash deposit options, and cooperation with the Federal Reserve and others in the cash handling industry, including armored cars vendors. Some consumers and merchants articulate important use cases for cash. The public policy questions surrounding merchants who choose to not accept cash are complex and emergent. We believe it is important for policymakers and merchants to engage in an authentic and ongoing dialogue about these issues.

As a sector which does not decide for merchants how they will accept payment, it would be difficult for us to use these written comments to address the myriad and quickly evolving questions raised by the decisions of some merchants to not accept cash. The implications for consumers and communities are important and we hope to learn from your work on this issue. While our sector recognizes the complexity

---

[17] *ibid.*

[18] Manuszak, M. and Wozniak, K. *The Impact of Price Controls in Two-Sided Markets: Evidence for US Debit Card Interchange Fee Regulation*. Federal Reserve Board, 2017

[19] *Out of Balance: How the Durbin Amendment has Failed to Meet Its Promise*. Electronic Payments Coalition, 2018

of the regulatory and legislative responses to merchants' decisions on payment acceptance, there are closely related policy matters which may bear in your consideration:

- **Merchants value electronic payments.** Mobile payments create exciting opportunities for merchants to increase engagement with their customers through promotions, repeat sales, and new options that improve their shopping cart conversion, like Buy Now Pay Later. The trend of cashless merchants in and of itself bears out what banks have known from decades of partnership with the retail sector: merchants who offer electronic payments do so because they provide some tangible business advantage over cash or checks. For some time, merchant trade associations have asserted that bank card acceptance is not competitively priced, and we offer the cashless trend as further evidence that card acceptance costs (interchange and related costs charged by banks to merchants) are reasonable.
- **Consumers value electronic payments.** When asked why they chose to pay electronically, consumers will cite a variety of reasons, including dispute rights, their ability to earn valuable rewards points or get cash back, easier tracking of expenses, avoiding counterfeit currency, or simply that they can replace a lost card more easily than cash.
- **Merchants make choices for their circumstances.** Excluding checks, cash was the only form of payment accepted by many merchants just a few decades ago. There was then, as there is now, a cost to accept, guard, and transport cash and unique risks associated with it (i.e. counterfeiting). Research shows that today, cash handling costs are at least as high as before electronic payments, and often exceed the cost of card acceptance. U.S. and Canadian retailers spent more than $96 billion in cash-handling activities in 2017.[20] For a variety of reasons, some merchants have chosen to introduce bank cards into their payments mix, some choose to remain cash-only, and some are now choosing to accept only non-cash payment types.
    - It is the experience of our industry that merchants actively manage their payment acceptance costs, balancing a number of factors as they seek to maximize their profitability. We know this most acutely because banks compete to serve merchants and offer them the best support for their choices. In fact, some merchants complain that they receive *too many* competing offers for payment services, stating that they are very satisfied with their current bank's services.
- **Mandates have consequences.** Merchant trade associations have long argued for heavy-handed government mandates on banks relating to card acceptance costs and practices. Despite evidence showing that merchants value electronic payments and receive benefits well above the price they pay to accept cards, a handful of merchant groups continue to seek government interventions ranging from mandating a 4-digit PIN (for purely their economic reasons) on all transactions to imposing price caps on card acceptance costs or routing requirements.

[20] *Cash Multipliers: How Reducing the Costs of Cash Handling Can Enable Retail Sales and Profit Growth.* IHL Group, 2018

Impact of Payments Mandates: the Debit Card Experience

As noted throughout our comments, the signature payments policy accomplishment of the retail lobby has been the Durbin Amendment, which raised financial services costs to consumers and reduced access to free checking and debit card rewards. We have and will repeatedly reference it because its impacts have so thoroughly rippled throughout a web of related issues, from delaying the rollout of secure payment technologies to touching on the most fundamental questions of competition and access. Regrettably, this law resulted in harm primarily to Americans of lower economic status while transferring tens of billions of dollars in benefits from consumers to large merchants, and harming the competitiveness of community financial institutions.

A recent Government Accountability Office report is the latest in a long line of studies outlining the negative consequences of the Durbin Amendment.[21] GAO highlighted several arguments that ABA has long held, including that the law significantly affected the cost and availability of basic banking services. For example, GAO cites a Federal Reserve study which found that noninterest checking account fees at covered banks rose by 20%, and the average minimum balance required to avoid a fee rose by 50% following the implementation of Reg II.[22] Market participants interviewed by GAO auditors also reported that the price cap "limited banks' ability to offer free checking accounts" (p. 25). Elsewhere in the report, GAO found that about 5% of U.S. households are unbanked, and nearly 18% are underbanked. Consumers who have lower incomes, lower socioeconomic attainment, or who are ethnic minorities are more likely to be unbanked or underbanked. Per GAO, unbanked individuals cite lack of funds, minimum balance requirements, and unpredictable or costly fees as the primary reasons for not having a bank account. As such, additional account fees and requirements—like those associated with interchange regulation—exacerbate the problem of unbanked and underbanked households.

We have long argued[23,24] that the Durbin Amendment represented a draconian, regressive step backwards for financial inclusion in basic banking services. Unheard of as an approach in the rest of the world, it was drafted without regular legislative order and passed without real debate. Regrettably, the Durbin Amendment has made it harder for people of modest means to obtain affordable bank accounts that include a bank-issued debit card. The recent dramatic reduction in card compensation for small banks attributable to Durbin suggests that this damage will continue to spread and impact more and more consumers as time goes on. It is impossible to ignore the reality that the cashless question would impact far fewer consumers if the Durbin Amendment had not passed and subsequently limited access to low- and no-cost debit cards.

---

[21] *Regulators Have Taken Actions to Increase Access, but Measurement of Actions' Effectiveness Could Be Improved.* GAO-22-104468. U.S. Government Accountability Office, 2022. https://www.gao.gov/assets/gao-22-104468.pdf

[22] See Manuszak and Wozniak. *The Impact of Price Controls in Two-sided Markets: Evidence from U.S. Debit Card Interchange Fee Regulation.* Federal Reserve Board, 2017. As cited in GAO-22-104468.

[23] *Don't be fooled: The Durbin amendment is a costly mistake*. Rob Nichols, President & CEO of the American Bankers Association. The Hill, 2017, https://thehill.com/blogs/pundits-blog/finance/330135-the-durbin-amendment-has-been-a-costly-policy-mistake-for-all

[24] Letter from the American Bankers Association, its State Associations, and Hundreds of its Members to the House of Representatives, for Repeal of Durbin Amendment. 2017. https://www.aba.com//media/documents/letterstocongressandregulators/finaldurbinletter.pdf?rev=bf714577884a49189f184846587cb868

Against that backdrop of reduced access to debit cards due to the merchant-driven Durbin Amendment, merchants now face the specter of a vastly different but similarly consequential mandate being placed upon their own payments acceptance practices. While you diligently examine the core aspects of the cashless question, we believe it is logical to consider seriously whether repealing the Durbin Amendment and restoring access to affordable basic banking services might become one prong of the Task Force's inclusion agenda.

Consumer Protection & Security in Mobile Payments

Technology and Security Standards Protect Consumer Privacy and Increase Access

In a competitive marketplace, standards evolve naturally through the interplay of marketplace, regulatory, and technological factors. In the payment space, banks abide both by voluntary private standards like those developed by EMVCo and the PCI Security Standards Council and government requirements such as data safeguarding rules resulting from the Gramm-Leach-Bliley Act. Payment brand policies are routinely updated to keep up with market realities – for example, many of us have noticed that card companies no longer require signing for card purchases (though some merchants still collect signatures for other reasons).

Banks work closely with regulators to understand best practices for keeping information safe. As chartered, regulated and insured institutions, banks are held accountable for protecting customer privacy, with specific limitations in place to prevent inappropriate data sharing.

Against this backdrop of strong government oversight, the private sector goes further by pursuing responsible growth of the payment system through new technologies while remaining eternally vigilant regarding data security. PCI and EMVCo form the foundation of a globally interoperable and secure payments system, with more opportunities than ever for participation by stakeholders in the merchant community. Often overlooked, private sector standards extend the use cases for mobile payments and pave the way for greater access.

In the age of the mega retailer data breach, banks continue to demonstrate an exceptional record of preventing data breaches. Combined with robust privacy protections, mobile payments made through a bank come with peace of mind that others cannot match.

Core Payment Systems Are Often Overlooked in Mobile Payments Debates

The networks which power mobile payments take a variety of forms. Payment card networks are the most ubiquitous connections between consumers' banks and a merchant's bank. These well-known brands provide for instant messaging of payment data around the globe, using globally-interoperable standards developed in formal consultations with merchants. The credit and debit card "rails" are a modern marvel: capable of processing the world's commerce with zero downtime and enabling transactions across borders in dozens of currencies. A debit card issued at a community bank in Philadelphia can be used in a mobile transaction in Tokyo or London because of private sector incentives for collaboration.

Automated Clearing House (ACH) networks are offering faster options that enable people to be paid more quickly and have access to their funds sooner than ever before. Of particular interest to policymakers concerned about families being able to make ends meet, data show that the use of Same Day ACH for payroll and other direct deposits increased by 105% between 2020 and 2021 (volume of funds processed

via same day settlement). About 95% of Americans now receive their paycheck via Direct Deposit,[25] allowing them to have access to funds on the morning of each payday. After hearing from stakeholders asking for faster access to funds for everyday Americans, banks stepped forward to create the *Real Time Payments* (RTP) network, a feature-rich interbank settlement system for faster payments. With RTP, banks and credit unions can instantly settle transactions made across innovative payment products, paving the way for the growth of new payment options. RTP is new kind of payment network based on the same technology used in the United Kingdom, Europe, and selected by central banks around the globe. The Federal Reserve is in a multi-year process of upgrading its payment offerings, including the rollout of their own real-time system, *FedNow*, at sometime next year.

The Interbank Model Protects Consumers and Communities; Direct Fintech Access is Dangerous

These core payment systems are key to the stability of our national economy and the operation of our government. For safety and system stability reasons, only chartered financial institutions and government agencies can access them, creating certainty for payment counterparties about the quality and liquidity of participants in the system. The interbank payments model protects consumers by providing them the assurance that their funds flow through a regulated, insured institution that is regularly examined for compliance with applicable laws. Further, banks are held to uniquely high standards for privacy, data security, community reinvestment, fairness, and preventing the facilitation of criminal activity such as human smuggling, human trafficking, and money laundering.

Standalone technology platforms and the retail sector are not subject to the above-stated obligations, nor are they specialists in managing the capital and risk calculations required to operate a sustainable payments business. Their financial structures are often geared towards research and development or inventory costs rather than meeting the stringent liquidity management practices required at banks. While some payment startups have been successful in injecting new ideas and competition into the ecosystem, there are also examples of elaborate and well-resourced end-to-end payment endeavors floundering. The mixed outcomes are no different than any other part of the tech sector.

Technology firms and retailers often partner with banks to offer mobile and other payment options because of, among other things, banks' access to the payments system, deep experience with payments, and extensive compliance and risk management systems. There are sound public policy reasons why the Federal Reserve, for instance, grants payment service accounts only to regulated banks and credit unions.

But there is a threat to this reliable and safe ecosystem. During the Federal Reserve's comments periods on proposals to upgrade their payment rails, some merchant groups and "big tech" interests (and academics) argued for direct access to these backbone systems.[26,27] This creates personal data privacy concerns for potential users of these big tech payment channels. Big tech has a history of mining transaction data from individuals for the purposes of targeted marketing or resale to third parties. Financial insitutions have strict

---

[25] *Getting Paid in America Survey.* National Payroll Week, 2021. https://www.nationalpayrollweek.com/wpcontent/uploads/2021/09/2021_Getting_Paid_In_America_survey_results.pdf

[26] Knight, B. *Fed Should Open the Payments System to Fintechs.* Mercatus Center, 2019. https://www.americanbanker.com/opinion/fed-should-open-the-payments-system-to-fintechs

[27] Hoenig, T. *FedNow Portents a More Competitive and Resilient Payments System.* Mercatus Center, 2019. https://www.mercatus.org/publications/monetary-policy/fednow-portends-more-competitive-and-resilient-payments-system

guard rails surrounding what they can do with customer data. Most tech companies and retailers do not seek direct access, recognizing that those sectors long ago left the finance space because of the complexity of participating directly. History shows that while major merchants (such as national department stores) originated the first credit cards, they sold their finance divisions to banks for sound business reasons.

For this reason, we are concerned about a potential shift in tone from the Federal Reserve, indicating an openness to offering new accounts to uninsured, nonbank providers. We understand the reasons why the House Financial Services Committee and Consumer Financial Protection Bureau are looking into the role of large tech platforms in payments and urge the Federal Reserve to observe longstanding policies which give these firms access through regulated channels.

America's Banks Are Working Together to Ensure Universal Access to Payment Choices

For payment networks to work, they need endpoints that reach everyone in the community. America's largest banks understand that and have sponsored the development of tools like RTP and mobile payment tools such as Zelle, for which they provide scale while simultaneously offering access on equal terms to smaller banks and credit unions. Our members are also proud to participate in advising the development of *FedNow*, along with other industries that have stakes in its rollout. Through engagement, small institutions have onramps to the latest payment highways that are being fed traffic by large institutions, building the networks to ubiquity. These products are arguably faster and superior to those developed outside the banking ecosystem because, when fully implemented, they do not require funds to sit with third parties before final settlement of transactions in a bank account. From large to small, the banking sector is working collaboratively to support the viability and sustainability of bank-based payment options.

Community Banks Still Face Unique Obstacles from Poor Technology Provider Choices

However, despite being offered the same technology as larger banks, community banks might still face the prospect of someday having comparatively fewer payment choices. The reason is straightforward: a heavily concentrated group of payment tech providers is failing to keep pace in supplying community banks with access to the best payment apps and online banking tools. Outdated software, poor hardware upgrade availability, and client support that has declined over the years combines to delay some small banks from adding new payment options. ABA members of all sizes are concerned about the impact of technological stagnation at so-called "core providers," especially in light of increasing consolidation – most recently the phenomena of payments processors merging with debit networks.

These Community Institutions Also Face Financial Pressure from the Durbin Amendment

The Federal Reserve recently documented that community banks and credit unions are experiencing sharp declines in interchange revenue, which is compensation received for providing a variety of services related to offering debit cards. While small institutions were supposed to be exempted from most of the Durbin Amendment's price caps on debit card transactions, they are still fully subject to some of the law's most prescriptive mandates. Further, the rules implementing the law deviated significantly from the statute by imposing mandates on financial institutions rather than prohibitions on conduct by payment networks. Neither of these outcomes are surprising given the unworkable design of the Durbin Amendment.

Unfortunately, by transferring revenue from banks to large retailers, the law has reduced the ability of smaller institutions to invest in offering the latest payment technology.[28]

Expanding the Durbin Amendment Would Compound This Harm

Mobile payments rely on robust underlying payment types. Attempts to expand the Durbin Amendment, either through the misguided Regulation II proposal now pending at the Federal Reserve Board, or through legislative expansion to credit cards, will most acutely harm community financial institutions that want to participate in digital and mobile payments platforms.

Digital Assets

Increasingly, consumers are accessing financial services through novel technologies like blockchain. What began with a single type of token (Bitcoin) has rapidly evolved into a complex and interconnected financial services ecosystem. Today, Pew estimates that 16% of U.S. adults have used cryptocurrency.[29] This quick evolution has created opportunities but has also challenged existing regulatory structures and introduced risk. Despite the decentralized origins of cryptocurrencies, the reality is that today most users access digital asset markets through (often large) centralized entities.

There is an increasing recognition of the importance of consistent regulation to ensure consumers remain protected when they engage with these novel assets. As Secretary of the Treasury Janet E. Yellen recently stated, "When new technologies enable new activities, products, and services, financial regulations need to adjust. But, that process should be guided by the risks associated with the services provided to households and businesses, not the underlying technology… Wherever possible, regulation should be 'tech neutral.' For example, consumers, investors, and businesses should be protected from fraud and misleading statements regardless of whether assets are stored on a balance sheet or distributed ledger." ABA agrees. We believe that consumers who choose to access crypto markets are best served when they can do so through a fully regulated financial institution like a bank. This consistent regulation is important in all assets but is critical for stablecoins. The stable nature of these assets mean they are marketed as an alternative to a bank deposit despite offering few of the protections consumers have come to expect from banks. This is why ABA supports the recommendations of the President's Working Group that stablecoin issuers be regulated as insured depository institutions.

Despite high-level agreement on the importance of the bank regulatory framework, it is becoming harder for regulated financial institutions like banks to offer their customers access to digital assets. The same day Janet Yellen gave her speech calling for more consistent regulation of digital assets, the FDIC issued a Financial Institution Letter (FIL) that made it more difficult for banks to offer crypto services. The FIL highlighted the risks of engaging in crypto activities and required banks engaged in any kind of crypto activity to seek prior approval from the FDIC. The FDIC is not alone – in November of 2021, the OCC issued

---

[28] *Joint Comments of the American Bankers Association, Credit Union National Association, and National Association of Federally-Insured Credit Unions to the Federal Reserve Board of Governors.* Docket: Regulation II Paperwork Reduction Act Information Collection, 2019.

[29] Perrin, A. *16% of Americans Say They Have Ever Invested In, Traded or Used Cryptocurrency.* Pew Research Center, 2021. https://www.pewresearch.org/fact-tank/2021/11/11/16-of-americans-say-they-have-ever-invested-in-traded-or-used-cryptocurrency/

Interpretive Letter 1179, which similarly required banks to obtain a written non-objection prior to engaging in activities deemed as permissible for banks in earlier interpretive letters.

The banking agencies are not alone in making it more difficult for regulated entities to meet customer demand for crypto services. Recently, the SEC published Staff Accounting Bulletin 121 which may require public companies to bring crypto assets held on a customer's behalf onto their balance sheet. Such a requirement would run counter to the longstanding bank business of safekeeping customer assets (e.g., book entry, physical, and digital assets) and would effectively bar banks from offering digital asset custody and related services.

If policymakers want consumers to be able to access digital assets through regulated financial institutions, they cannot at the same time tell regulated financial institutions not to offer these products. All that will accomplish is pushing non-bank providers and consumers farther from fully regulated markets, exposing them to undue risk.

Policy Recommendations

We urge the Task Force to consider the following public policy priorities on mobile payments:

- **Support the Withdrawal of Regulation II Expansion.** The Federal Reserve Board should withdraw its 2021 Proposed Rule to expand the Durbin Amendment to virtually any kind of debit card transaction, a standard which is so vague and confusing that it threatens to undermine key parts of the mobile wallet ecosystem. Its implicit endorsement of a mandate that community financial institutions accept so-called "PINless" transaction types would fundamentally transform the payments system in a manner not required by Congress, while removing card issuer discretion in preventing fraud – a harsh blow to small banks and credit unions operating payment systems on tight margins. The Proposed Rule was issued without the analyses required by law, including regarding the impacts on small entities. Once withdrawn, it should only be reproposed after all procedural requirements are satisfied and its substantive flaws remedied, and if the Federal Reserve can articulate a compelling justification for continuing to pursue this discretionary rulemaking at the expense of small financial institutions and their customers.

- **Proceed Cautiously With Large Scale Rewiring.** The payments system is complex and has evolved to meet needs of an economy that requires specialized solutions. The urge to start from scratch can lead to unintended consequences. Instead, we urge policymakers to support those prudently-planned fresh starts like the real time payment systems being introduced by the private sector and the Federal Reserve that clear the clutter from transactions and empower new use cases for mobile payments. These solutions are arriving much sooner than a CBDC could. Similarly, radically expanding direct access to the nation's core payment systems would create downside risk without any clear benefit to the economy.

- **Ensure Consistent Expectations.** Bank and nonbank providers should be held to similar standards for consumer protection, security, and liquidity. Mobile payment providers should be subject to common regulatory baselines and we urge Congress to exercise oversight of attempts to circumvent safeguards that consumers have come to expect. No matter where payment-related data flows, it should be protected by the same standards. Nonbanks also should not be able to create moral hazard by operating business models that pool risk and potentially introduce instability into the nation's backbone payment systems.

- **Support Innovation by Regulated Financial Institutions.** For new payment types like crypto to become safe and commonly accepted mobile payments, banks must have consistent guidance from regulators that does not put them at a disadvantage to lesser regulated competitors. Current regulations hamstring banks by requiring and withholding non-objections, making it difficult for customers to access digital assets. We urge Congress to monitor actions by regulators that prevent the kind of harmonization of expectations that would create a predictable, regulated marketplace for new assets.

Conclusion

Once again, ABA appreciates the opportunity to offer this statement for the record and to contribute to the dialogue undertaken by the Task Force. We remain at your disposal to answer your questions and provide further information. ABA looks forward to more Task Force hearings on payments issues in the future.

What's in Your Digital Wallet?

A Review of Recent Trends in Mobile Banking and Payments

House Financial Services Taskforce on Financial Technology

Thursday April 28, 2022

Statement for the Record

of

Consumer Federation of America

National Consumer Law Center
on behalf of its low-income clients

National Consumers League

U.S. PIRG

Chairman Lynch, Ranking Member Davidson, and Members of the Taskforce:

Consumer Federation of America, the National Consumer Law Center, on behalf of its low-income clients, the National Consumers League and U.S. PIRG submit the following statement for the record in connection with the Taskforce's hearing on What's in Your Digital Wallet? A Review of Recent Trends in Mobile Banking and Payments.[1]

This statement focuses on digital wallets such as PayPal's Friends & Family and Venmo services and Block's Cash App, and similar person-to-person (P2P) services like Zelle, which is used between bank accounts. We draw attention to two concerns about these services.

First, there is a profound need for more consumer protection against fraud and errors in payments made through digital wallets and other peer-to-peer (P2P) services. Payment services and financial institutions must take more responsibility to protect consumers from the fraud committed on their platforms and the scammers they allow to open accounts where they can receive stolen funds.

We support the discussion draft of the Protecting Consumers From Payment Scams Act, which would address many gaps and ambiguities in the Electronic Fund Transfer Act that leave consumers unprotected.

Second, all deposit accounts should be required to carry deposit insurance to ensure that funds are safe. Yet today, digital wallets offered by nonbank entities hold billions in consumers' funds on their own books without insurance. PayPal alone holds nearly $40 billion in uninsured funds and Block's Cash App holds about $4 billion. Congress or the Department of Justice should take action to require those and other deposit accounts that hold consumer funds to carry deposit insurance.

This statement will not address the privacy issues posed by digital wallets, but we agree with others that any data collected through payment systems should be used only with consumer permission and in ways that they would expect. And we repeat our call for the Consumer Financial Protection Bureau (CFPB) or Congress to make clear the application of existing federal data governance laws, including the Gramm-Leach-Bliley Act (GLBA) and the Fair Credit Reporting Act (FCRA), to P2P services.[2]

I. Consumers should be protected from fraud in the inducement in P2P services connected to both digital wallets and bank accounts.

A. Fraud is a growing problem in P2P services

As consumer, small business, civil rights, community, and legal service groups described at greater length in comments submitted last year to the Federal Reserve Board and the Consumer Financial Protection Bureau, the existing P2P payment systems of large technology companies and financial institutions simply are not safe for consumers to use.[3]

---

[1] These comments were written by Lauren Saunders and Carla Sanchez-Adams at the National Consumer Law Center.

[2] *See* Comments of 65 Consumer, Civil Rights, Faith, Legal Services and Community Groups to CFPB on Big Tech Payment Platforms at 4-5, Docket No. CFPB-2021-0017 (Dec. 21, 2021), https://bit.ly/CFPB-BTPS-comment ("CFPB Big Tech Payment Platform Comments").

[3] *Id.*; Comments of 43 consumer, small business, civil rights, community and legal service groups to Federal Reserve Board Re: Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers

The Federal Trade Commission (FTC) received nearly 2.8 million fraud complaints in 2021, totaling nearly $6 billion in reported losses.[4] Yet that number that vastly understates total fraud losses, as many frauds go unreported.

The top payment method used by scammers to obtain funds, in terms of dollars lost, is now "bank transfer or payment."[5] Reported losses in that category in 2021 more than doubled from the previous year.[6] Losses from scams paid through "payment app or service" also increased by nearly 50% over 2020.[7] The CFPB has also seen high growth in complaints about fraud in digital wallets.[8]

Scams can have a particularly harsh impact on low-income families and communities of color. Scams often take the last dollar from those least able to afford it, and often target older adults, immigrants, and other communities of color.[9] These communities, already denied or stripped of wealth through discrimination over the centuries to the present day, can least afford to lose money to scams and errors. P2P payment systems, if properly designed, can provide broad benefits to consumers. But those benefits will only be realized if the systems are safe to use.

Fraud losses are directly linked to the rapid growth of P2P services, which are used by tens millions of people, allow payments to be sent at very low or no cost between consumers or from consumers to businesses.[10] An astounding 79% of Americans use mobile payment apps.[11] But as the usage has climbed in recent years, so have the complaints.

Approximately one quarter of the payment app complaints to the CFPB in 2020 related to scams, with about the same number tied to unauthorized transactions or other transaction problems. These problems are escalating because the current payment app systems impose no requirements on the system operators to protect consumers against fraud and common errors. Given what we know about how scammers target opportunities with the least resistance, it stands to reason that fraud and errors will continue to plague P2p systems if financial institutions

---

Through Fedwire, Docket No. R-1750; RIN 7100-AG16 (Sept. 9, 2021), https://bit.ly/FedNowCoalitionComments ("FedNow Comments").

[4] https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0.

[5] FTC, Fraud Reports by Payment Method, https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/LossesContactMethods.

[6] *Id.* In 2021, $756.5 million in losses from bank transfer or payment were reported, compared with $321.3 million in 2020. However, only 16% of reported losses disclosed the payment method, so those numbers vastly understate total losses.

[7] *Id.*

[8] U.S. PIRG Educ. Fund, Virtual Wallets, Real Complaints 2 (June 2021), *available at* https://uspirg.org/sites/pirg/files/reports/VirtualWallets/Virtualwallets_USP_V3.pdf.

[9] Anthony Hill, ABC Action News, "In-depth: Top scams that are targeted against the Black community; how to avoid falling victim; 41% of African Americans say they were targeted by a scam" (Aug. 12, 2021); https://www.abcactionnews.com/news/in-depth/in-depth-top-scams-that-are-targeted-against-the-black-community-how-to-avoid-falling-victim; Josh McCormack, Salud America, "Scammers Target Latinos, Blacks More Than Other Groups" (Aug. 31, 2021), https://salud-america.org/scammers-target-latinos-blacks-more-than-other-groups/; Matthew Petrie, AARP, Consumer Fraud in America: The Latino Experience (Aug. 2021), https://www.aarp.org/research/topics/economics/info-2021/scam-experiences-hispanic-latino.html.

[10] Alexander Kunst, Statista Global Consumer Survey (Nov. 19, 2020), *available at* https://www.statista.com/forecasts/997123/peer-to-peer-payments-in-the-us.

[11] U.S. PIRG Educ. Fund, Virtual Wallets, Real Complaints 2 (June 2021), *available at* https://uspirg.org/sites/pirg/files/reports/VirtualWallets/Virtualwallets_USP_V3.pdf.

are allowed to operate under the assumption that they are not liable for fraud in the inducement or sender errors.

The news media has reported many of the scams that were enabled by the P2P systems. Generally, these scams would not have been possible without the payment apps.

- Luke Krafka, a professional musician in Long Island, lost almost $1,000 dollars through Zelle when a fake client "hired" him to play at a wedding. The man sent him a large check and asked him to pay part of the money back through Zelle. The check bounced after Krafka had already sent the money. His bank refused to refund his payment.[12]

- Mary Jones of Kansas City paid $1,700 through Venmo in "rent" to a man who claimed to own the house she wanted to move into. He even gave them access to tour the house before she signed the lease. After she saw a For Lease sign in the front yard, she called the rental company and discovered that she had paid a scammer. She filed a police report but has not been able to retrieve her money.[13]

Scammers have extraordinary creativity. They are constantly developing creative ways to steal people's money. The Federal Communication Commission's website includes a Scam Glossary detailing dozens of different ways individuals and small businesses have lost money to scams.[14] The FTC specifically identified P2P apps as a primary means for executing these scams.[15] Clearly, the warnings provided by the payment apps themselves to beware of scams are not adequate to protect consumers from the losses.

These P2P scams are likely to skyrocket even more after the FedNow service – which, like Zelle, will operate between banks, but may have an even broader reach – launches. Unfortunately, the currently proposed rules leave consumers exposed to fraud and errors with little recourse.[16]

B. Payment services and financial institutions have an obligation to take more responsibility when they enable scammers to receive funds

Payment system providers can do far more to protect consumers, and ultimately the systems themselves will benefit if consumers have greater protection and confidence when making person-to person (P2P) payments.

The providers of these P2P systems make decisions about what safety features to install, when to protect consumers, and how to monitor and react to red flags of potentially fraudulent payments received by their customers. Unfortunately, these companies have made the decision to prioritize speed, convenience, and ubiquity at the expense of safety. They must instead take responsibility

---

[12] *See* CBS This Morning, *Complaints against mobile payment apps like Zelle, Venmo surge 300% as consumers fall victim to more money scams*, CBS News (June 23, 2021), *available at* https://www.cbsnews.com/news/venmo-payal-zelle-cashapp-scams-mobile-payment-apps/.
[13] Tia Johnson, *Kansas City woman warns others after losing nearly $2,000 in rental home scam*, Fox4 (May 3, 2021), *available at* https://fox4kc.com/news/kansas-city-woman-warns-others-after-losing-nearly-2000-in-rental-home-scam/.
[14] Federal Commc'ns Comm'n, Scam Glossary, *available at* https://www.fcc.gov/scam-glossary.
[15] Federal Commc'ns Comm'n, As More Consumers Adopt Payment Apps, Scammers Follow (updated Feb. 25, 2021), *available at* https://www.fcc.gov/more-consumers-adopt-payment-apps-scammers-follow.
[16] *See* Comments of National Community Reinvestment Council, National Consumer Law Center, National Consumers League re: Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire, Docket No. R-1750, RIN 7100-AG16 (Sept. 9, 2021), https://bit.ly/FedNowNCLC-NCRC-NCL.

for their choices and protect consumers when the systems they design and implement result in predictable errors or fraud.

Protecting consumers from errors and fraud will create greater incentives for payment system providers to prevent those problems in the first place, benefiting everyone. Getting those incentives right is critical, as companies that are incentivized to prevent fraud and errors will use constantly improving technology and innovations to spot potential scams and errors, aggregate reports of fraud, and freeze accounts that are being used to receive fraudulent funds before the funds are gone and before more consumers can be defrauded.

In today's world of fintech and innovation, it is ironic that the payment system providers' primary response to fraud and errors in P2P systems is to use old-fashioned disclosures and warnings to consumers to "be careful" and not to send payments to people they do not know -- even while promoting their systems for broad use. Scammers prey on consumers' trust, and warnings are far less effective than the sophisticated systems that payment providers can design.

It is especially important to flag the responsibilities of the institution that holds the account that receives a fraudulent payment. Institutions already have the duty to know their customer and to monitor accounts to prevent illegal activity. When they fail in those responsibilities and allow a customer to use an account that enables a scam, it is appropriate for that institution to bear the costs if the funds cannot be recouped.

If fraud and error rates are low in the aggregate, the system can bear those costs and spread them. If rates are high, then the systems clearly have fundamental problems that must be addressed. But even a single instance of fraud or mistake can be devastating to a consumer. The equities strongly favor protecting consumers with the same type of strong protection they have in the credit card market.

C. Current interpretations of the EFTA do not protect consumers from payment scams

In its current form and as interpreted and implemented by financial institutions, Regulation E—the regulation that implements the Electronic Fund Transfer Act (EFTA)--does not provide adequate protections to consumers in P2P push-payment systems like those used through digital wallets or through bank account services like Zelle. If the consumer initiated the transfer, financial institutions are likely to dispute their liability and may even refuse to help.

The EFTA was enacted 43 years ago and does not directly address many of the most important issues in the current consumer payment ecosystem. The statute was initially adopted at a time when consumers were conducting business with their own financial institutions and were using payment systems that did not lead to the same types of problems that plague today's P2P systems.

Regulation E gives consumers protection from unauthorized transfers, but the definition of "unauthorized transfer" is a transfer from a consumer's account "initiated by a person *other than the consumer* without actual authority to initiate the transfer and from which the consumer receives no benefit."[17] Thus, Regulation E's protection against unauthorized transfers will likely not apply when the consumer is fraudulently induced to make a payment, even if the consumer's authorization was obtained through fraud.

[17] 12 C.F.R. § 1005.2(m) (emphasis added).

There is little difference between these two scenarios:

- *Scenario A: Laurie receives a call from a person claiming to be with the IRS. The caller threatens to arrest her if she does not make a payment. Laurie gives the caller her bank account number and routing number, and the caller uses that information to initiate a preauthorized ACH debit against her account.*

- *Scenario B: Laurie receives a call from a person claiming to be with the IRS. The caller threatens to arrest her if she does not make a payment. Laurie takes out her smartphone and sends a P2P payment to the number or email given by the caller.*

The only difference between these two scenarios is that in the second Laurie was the person that took the first step in the payment system to initiate the payment. That difference does not make the scammer any more entitled to the money **or make the scammer's bank any less responsible for banking a scammer**. Yet in the first scenario, Regulation E protects Laurie, and she could contest the debit as unauthorized, whereas in the second, financial institutions take the position that she is unprotected because she initiated the payment.

Indeed, the first scenario is unlikely, because scammers like the fake IRS caller would likely not use the ACH system. The ACH system vets and monitors who is allowed to initiate ACH payments, and the liability of a bank that initiates and receives fraudulent debit payments under both Regulation E and NACHA rules leads to stronger controls that are more likely to keep the scammer from having an account or having access to the ACH system.

But with digital wallets and online bank account opening and identity theft, it is easier for scammers to obtain accounts – potentially using stolen identities – that they can use to receive payments (directly or through money mules). Yet the receiving bank has no liability for enabling the scammer to receive the payment, giving the bank less incentive to prevent the scammer from having an account, to put a hold on access to suspicious payments, or to shut down the account quickly.

D. Lessons from the United Kingdom show how everyone benefits when consumers are protected from fraud – but protection must be required, not voluntary

1. The UK Contingent Reimbursement Model Code

The United Kingdom was early to launch real time payments, and payment fraud immediately followed. The UK has been formally considering how to tackle the problem of P2P fraud since 2016, when the consumers association "Which?"[18] submitted a "super-complaint"[19] to the United Kingdom's Payments Systems Regulator (PSR).[20] The complaint identified the problem of

[18] The Treasury has the power to designate certain bodies as super-complainants to the Payment Systems Regulator, and Which? is one of these groups. https://www.gov.uk/government/publications/super-complainants-for-the-payment-systems-regulator.

[19] A super-complaint may be made by a designated consumer body where the body considers features of a market in the United Kingdom for payment systems that are or which may be significantly damaging to the interests of consumers. https://www.gov.uk/government/publications/super-complainants-for-the-payment-systems-regulator.

[20] As part of the Financial Services (Banking Reform) Act of 2013, the Payment Systems Regulator (PSR) was established to promote competition, innovation, and responsiveness of payment systems and to receive and respond to super-complaints. https://www.gov.uk/government/publications/super-complainants-for-the-payment-systems-regulator.

authorized push payment fraud (APP fraud), which happens when scammers deceive consumers or individuals at a business to send them payment under false pretenses to an account controlled by the scammer. Which? also identified the lack of consumer protection for victims of APP fraud.

As a result, a steering group was formed, comprised of regulators, consumer advocates, financial services providers and industry representatives.[21] The result was the creation of an industry code called the Contingent Reimbursement Model (CRM) Code, launched in 2019, which requires signatories to reimburse consumers who are the victims of APP fraud under certain circumstances.[22] The CRM Code is voluntary and exists to help financial institutions in the UK "detect, prevent and respond to APP scams."[23]

The voluntary decision of the leading UK payment industry players to develop a system to reimburse fraud victims shows the consensus that protecting consumers benefits industry players and the payment systems as a whole, not merely consumers. But the uneven implementation of the system – and growing calls to make it mandatory – also show the limits of voluntary measures.

The CRM Code "sets out consumer protection standards to reduce APP scams, which occur when customers are tricked into authorizing a payment to an account they believe belongs to a legitimate payee."[24] UK banks and building societies (akin to credit unions in the U.S.) recognize the need to address the rising costs of APP fraud. The Lending Standards Board (LSB), the primary self-regulatory body for the banking and lending industry in the United Kingdom,[25] monitors and updates the CRM Code.

There are currently 18 signatories to the CRM Code:

Bank of Scotland plc
Barclays
Cahoot
Cater Allen Limited
Co-op Bank
First Direct
Halifax
HSBC
Intelligent Finance
Lloyds Bank
M&S Bank
Metro Bank
Nationwide Building Society
NatWest
Royal Bank of Scotland plc
Santander
Starling Bank
Ulster Bank[26]

---

[21] https://www.lendingstandardsboard.org.uk/scams-looking-forward-priorities-and-opportunities-international-perspective-speech/.
[22] *Id.*
[23] https://www.lendingstandardsboard.org.uk/scams-looking-forward-priorities-and-opportunities-international-perspective-speech/.
[24] https://www.lendingstandardsboard.org.uk/crm-code/ .
[25] https://www.lendingstandardsboard.org.uk/who-we-are/ .
[26] *See* Which?, "What to do if you're the victim of a bank transfer scam" (updated Mar. 14, 2022),

Each signatory commits to various measures to prevent APP fraud as outlined in the Code.[27] These measures include setting up systems and processes to implement the requirements of the Code; detect and prevent fraud; train employees who handle disputes and customer service complaints about APP fraud; track data about Code compliance and adjust policies as needed in response to the data; provide warnings to customers about scams and potential fraud; provide Confirmation of Payee services; and timely respond to consumer complaints.[28] As LSB Chief Executive Emma Lovel stated:

> "[Signatory banks and other financial services firms] have committed to:
>
> - take steps to educate their customers about APP scams;
> - identify higher risk payments and customers who have an increased risk of becoming a victim of a scam;
> - provide effective warnings to customers if the bank identifies an APP scam risk;
> - take extra steps to protect customers who might be vulnerable to APP scams;
> - talk to customers about payments and even delay or stop payments where there are scam concerns;
> - act quickly when a scam is reported;
> - take steps to stop fraudsters opening bank accounts; and
> - *reimburse customers who lose money where they were not to blame for the success of a scam."*[29]

The CRM Code establishes the required timelines for investigating and resolving a claim of APP fraud[30] as well as the factors to consider in determining whether a consumer should be reimbursed for the amount of the APP fraud.[31] The Code instructs firms to reimburse victims of APP fraud unless the firm can establish that their customer did not have a reasonable basis for believing that the person or organization they are sending money to is legitimate, [32] or the victim was grossly negligent[33] or acted dishonestly or obstructively in a material respect.[34]

The Code also provides for division of the costs of reimbursing a defrauded consumer between the consumer, the sending financial institution, and the receiving institution, in light of whether the

---

https://www.which.co.uk/consumer-rights/advice/what-to-do-if-you-re-the-victim-of-a-bank-transfer-app-scam-aED6A0l529rc#if-your-bank-is-signed-up-to-the-code.

[27] *Id.*

[28] https://www.lendingstandardsboard.org.uk/wp-content/uploads/2022/03/CRM-Code-LSB-April-2021.pdf

[29] https://www.lendingstandardsboard.org.uk/scams-looking-forward-priorities-and-opportunities-international-perspective-speech/ (emphasis added).

[30] R3, R4 at p. 16-15, Contingent Reimbursement Model Code for Authorised Push Payment Scams, 20 April 2021 found at https://www.lendingstandardsboard.org.uk/wp-content/uploads/2022/03/CRM-Code-LSB-April-2021.pdf

[31] R1, R2 at p. 14-15, Contingent Reimbursement Model Code for Authorised Push Payment Scams, 20 April 2021 found at https://www.lendingstandardsboard.org.uk/wp-content/uploads/2022/03/CRM-Code-LSB-April-2021.pdf

[32] R1, R2(1)(c) at p.14, Contingent Reimbursement Model Code for Authorised Push Payment Scams, 20 April 2021 found at https://www.lendingstandardsboard.org.uk/wp-content/uploads/2022/03/CRM-Code-LSB-April-2021.pdf

[33] R2(1)(e) at p.14, Contingent Reimbursement Model Code for Authorised Push Payment Scams, 20 April 2021 found at https://www.lendingstandardsboard.org.uk/wp-content/uploads/2022/03/CRM-Code-LSB-April-2021.pdf

[34] R2(2)(b) at p.14, Contingent Reimbursement Model Code for Authorised Push Payment Scams, 20 April 2021 found at https://www.lendingstandardsboard.org.uk/wp-content/uploads/2022/03/CRM-Code-LSB-April-2021.pdf

institutions complied with provisions of the Code and whether the consumer met the requisite level of care as defined in the Code.[35]

A consumer who is not satisfied with the resolution of a fraud claim can raise a case with the Financial Ombudsman Service.

2. The voluntary nature of the CRM Code has hampered its effectiveness.

The development of the CRM code is laudable, and it has resulted in compensation for some scam victims. Unfortunately, that is a drop in the bucket, and the voluntary nature of the code has led to wide failures to comply, even among those pledged to abide by it. As a result, the UK's payments regulator is working on changes to provide for mandatory reimbursement for scam victims.

As reported in September 2021, very few victims of APP fraud were reimbursed under the CRM Code: "banks found victims at least partly responsible in 77% of cases assessed in the first 14 months following the introduction of a Contingent Reimbursement Model and voluntary code."[36] Two banks found the customer fully liable in 90% of their decisions.[37]

Under the CRM code, consumers who are unhappy with their bank's refusal to compensate them can appeal to the Financial Ombudsman Service, which reviews denials of reimbursement requests for APP fraud. Data obtained by Which? found that the ombudsman concluded that banks were getting the decisions wrong, finding in favor of a consumer in 73% of the complaints about APP fraud it received from 2020-2021.[38] This level of reversals suggests that the banks' high rate of denials is inconsistent with both the letter and the spirit of the Code.[39]

The Contingent Reimbursement Model as an industry response, though laudable and necessary, has proven insufficient to address the growing number of scams and fraud. In the first half of 2021, APP fraud cases in the UK outnumbered credit card fraud for the first time.[40]

In response to this continued problem of APP fraud, John Glen, economic secretary to the Treasury stated of the Government's position:

> "Liability and reimbursement requirements on firms need to be clear so that customers are suitably protected. It is welcome that the Payment Systems Regulator is consulting on measures to that end, and to help prevent these scams from happening in the first place. The Government will also legislate to address any barriers to regulatory action at the

---

[35] ALL1, ALL2, ALL3 at p. 17-18, Contingent Reimbursement Model Code for Authorised Push Payment Scams, 20 April 2021 found at https://www.lendingstandardsboard.org.uk/wp-content/uploads/2022/03/CRM-Code-LSB-April-2021.pdf

[36] https://www.finextra.com/newsarticle/38832/banks-called-to-account-over-shockingly-low-rate-of-reimbursements-for-app-fraud

[37] *Id.*

[38] Which?, "Banks wrongly denying fraud victims compensation in up to 8 in 10 cases" (Nov. 11, 2021), https://www.which.co.uk/news/2021/11/banks-wrongly-denying-fraud-victims-compensation-in-up-to-8-in-10-cases/.

[39] Contingent Reimbursement Model Code for Authorised Push Payment Scams OP1 at 2, (Apr. 20 2021), https://www.lendingstandardsboard.org.uk/wp-content/uploads/2022/03/CRM-Code-LSB-April-2021.pdf

[40] "UK Government to Legislate for Mandatory Reimbursement of App Fraud," November 18, 2021, available at https://www.finextra.com/newsarticle/39245/uk-government-to-legislate-for-mandatory-reimbursement-of-app-fraud

earliest opportunity."[41]

The UK Parliament's Treasury Committee has recommended "mandatory refunds" to victims of APP fraud and discussion about whether to make "big technology companies liable to pay compensation when people are tricked by con-artists using their platforms."[42]

The Payment Systems Regulator (PSR) is also undertaking rulemaking. As part of the PSR's proposed rules, UK banks will be "required to publish data on their performance in relation to APP scams, on reimbursement levels for victims, and which banks and building societies' accounts are being used to receive the fraudulent funds."[43] Additionally, Chris Hemsley, managing director of the PSR, states:

> "[W]e are also setting out the way to make reimbursement mandatory for those blameless victims so that, when the law is changed, we are ready to act as quickly as possible to get protections to the people who need them."[44]

E. Other gaps and ambiguities that hamper the effectiveness of EFTA's protection for P2P services

In addition to the lack of protection when consumers initiate payments to scammers, there are other gaps, ambiguities or disagreements about the EFTA's protections that can leave consumers unprotected when problems arise with digital wallets and P2P services.

1. Bank wire transfers are exempt from the EFTA, leaving consumers exposed to losing tens of thousands of dollars.

The EFTA exempts electronic transfers, other than ACH transfers, made "by means of a service that transfers funds held at either Federal Reserve banks or other depository institutions and which is not designed primarily to transfer funds on behalf of a consumer."[45] Regulation E and the official interpretations of Regulation E interpret that exemption to cover wire transfers using FedWire, SWIFT, CHIPS and Telex[46] – that is to say, virtually all wire transfer services used by banks.

Thus, even if a criminal impersonates the consumer and makes a completely unauthorized wire transfer, the consumer may have no protection under Regulation E. The transfer would be covered under state law by UCC Article 4A, but that article was designed for commercial-to-commercial transactions and has far weaker protections than the EFTA.

In just the last few months, the National Consumer Law Center has received several inquiries

---

[41] *Id.*
[42] "Fraud: MPs seek overhaul to tackle financial scammers," February 2, 2022, available at https://www.bbc.com/news/business-60216076.
[43] UK Government to Legislate for Mandatory Reimbursement of App Fraud," November 18, 2021, available at https://www.finextra.com/newsarticle/39245/uk-government-to-legislate-for-mandatory-reimbursement-of-app-fraud
[44] *Id.*
[45] 15 U.S.C. §1693a(7)(B).
[46] 12 C.F.R. §1005.3(c)(3) (exempting FedWire or similar systems); Official Interpretation of 3(c)(3)-3 ("Fund transfer systems that are similar to Fedwire include the Clearing House Interbank Payments System (CHIPS), Society for Worldwide Interbank Financial Telecommunication (SWIFT), Telex, and transfers made on the books of correspondent banks.").

on behalf of consumers who have lost thousands of dollars due to unauthorized wire transfers:

- A college student lost his entire savings account after someone with two fake identification cards went into a bank and wired $16,500 to another individual. Busy with college, he did not notice missing money for a month and a half – still within the EFTA time frame for disputing it – but the bank refused to return the money.[47]

- After a consumer was the victim of a SIM swap, a wire transfer was used to transfer $35,000 from his bank account to an account in another state.[48] He is a cancer patient and navigating the bank appeal process has been extremely stressful. These SIM swaps are increasingly common.[49]

- A low-income consumer in New York lost over $26,000 – all of her savings, which she had carefully saved over many years -- after someone transferred money from her checking account to her savings account, and then made an outgoing wire transfer to another state.[50]

- A man lost $15,000 that was wired to another account by someone who gained access to his account. The bank spotted suspicious activity as the fraud was taking place and called the man, who alerted them to the fraud, but the bank still refused to return the money, claiming that the EFTA did not apply to these fraudulent electronic transactions.

- A fraudster hacked a retiree's online banking account and made a cash advance from the retiree's credit card to his linked bank account. The fraudster then immediately wired that amount from the retiree's bank account to his own. The bank denied any relief.[51]

- A small business had its online banking account hacked and its $60,000.00 checking account balance emptied over the course of two days and six transactions. The bank denied relief because its banking agreement generally states that customers are responsible for unauthorized transactions.[52]

The precise reasons why the banks in all of these situations refused to reverse the unauthorized transfers are not quite clear. But the fact that these transfers may be exempt from the EFTA exposes a dramatic gap in protection that is causing severe harm.

2. **Consumers' accounts may be frozen or closed, leaving them unable to access their funds for weeks or months**.

Another ambiguity or matter of dispute is what recourse consumers have if a bank or payment app freezes or closes their account, refusing to release the money or holding it for an extended period of time.
Banks and payment apps sometimes have reasons to freeze or hold accounts, especially if they

[47] Inquiry received by KPRC (Houston NBC station) reporter Amy Davis.
[48] Email from attorney on file with NCLC.
[49] *See* Luke Barr, ABC News, "'SIM swap' scams netted $68 million in 2021: FBI" (Feb. 15, 2022), https://abcnews.go.com/Politics/sim-swap-scams-netted-68-million-2021-fbi/story?id=82900169.
[50] Email from CAMBDA Legal Services to NCLC, on file with NCLC.
[51] Pending arbitration before AAA (Wells Fargo).
[52] Lawrence and Louis Company d/b/a Hidden Oasis Salon v. Truist Bank, No. 1:22-cv-200-RDA-JFA (E.D. Va.).

suspect that the accountholder has committed fraud or used a stolen identity.

But financial institutions have at times overreacted to fraud waves, catching innocent consumers in the process. Often, the most vulnerable people have been denied access to their money.

If the consumer is unable to make an electronic withdrawal or transfer, that should be viewed as an error triggering the error resolution rights, duties, timelines and investigation procedures of the EFTA. But banks and payment apps seem to believe the EFTA does not apply in this situation.

After Chime embarked on a marketing campaign to convince people to open up Chime accounts to receive their stimulus payments, its inadequate identity verification led to a wave of fraud. Chime then froze numerous accounts, leaving some people without their money for months on end:

- "Chime stole my entire unemployment backpay…. I'm a single mom of 4 kids and they stolen $1400 from me and refuse to give it back and now we are about to be evicted."[53]

Similarly, Bank of America froze 350,000 unemployment debit cards in California after extensive fraud reports. But the freezes caught many legitimately unemployed workers and the bank failed to respond in a timely fashion to their complaints:

- "Heather Hauri got a text from Bank of America that suggested her debit card may have been compromised too. When she responded that she had not made the transactions in question, she was locked out of her account. 'The whole account is frozen,' she said. 'You can't get your own money.'"[54]

Months later, after a lawsuit was filed, a judge prohibited the bank from freezing accounts for California unemployment benefits based solely on an automated fraud filter and required it to do a better job of responding when jobless people say their benefits were stolen.[55]

3. **Payment apps and bank P2P services make it easy for consumers to make errors, but leave people with no protection.**

Finally, payment apps and financial institutions typically refuse to help when consumers accidentally send money to the wrong person or the wrong account – mistakes that are easy to make in payment services designed for convenience and speed over safety. Regulation E imposes the duty to investigate and resolve "errors," which includes "an incorrect electronic fund transfer to or from the consumer's account."[56]

Nothing in the EFTA excludes consumer errors, and Regulation E should be interpreted to cover them. When a payment is sent to the wrong person or in the wrong amount, the person receiving the payment is not more entitled to the payment because the error was caused by the sender. But today, most consumers are out of luck in this situation unless their bank decides to help them and

[53] Carson Kessler, ProPublica, "A Banking App Has Been Suddenly Closing Accounts, Sometimes Not Returning Customers' Money" (July 6, 2021), https://www.propublica.org/article/chime.
[54] Bank Of America Freezes EDD Accounts Of Nearly 350,000 Unemployed Californians For Suspected Fraud (Oct. 29, 2020), https://www.cbsnews.com/losangeles/news/bank-of-america-freezes-edd-accounts-of-nearly-350000-unemployed-californians-for-suspected-fraud/.
[55] Patrick McGreevy, Los Angeles Times, "Bank of America must provide more proof of fraud before freezing EDD accounts, court orders" (June 1, 2021), https://www.latimes.com/california/story/2021-06-01/bank-of-america-ordered-to-unfreeze-unemployment-benefit-cards-in-california.
[56] 12 C.F.R. §1005.11(a)(1)(ii).

the receiving bank or payee is cooperative.

Here are a couple of examples:

- An employee of NCLC unexpectedly saw $1,000 arrive in his bank account through Zelle. A few minutes later, he received a frantic phone call from a man telling him that he had put in the wrong cell phone number and asking for the money back. The NCLC employee wanted to return the money but asked his bank for assurances that it was not a scam. The man also called his bank. Both banks (both large top-10 institutions) refused to help correct the error. After weeks of getting nowhere, the NCLC employee returned the funds on faith.

- Arthur Walzer of New York City tried to send his granddaughter $100 through Venmo as a birthday present, but instead sent it to a woman with the same first and last name. When he discovered the error, he told his bank to refuse payment of the $100, and in response Venmo froze his account and demanded that he pay them. Venmo eventually refunded him, but only after a journalist contacted the company on his behalf. It was the first time he had ever used Venmo – he set up an account specifically to give his granddaughter the gift.[57]

Errors are easy to make in today's P2P systems. For example, today consumers can send money through P2P systems using nothing more than a cell phone number to identify the recipient.

Banks are also refusing to correct errors that arguably were committed by a bank, not the consumer. For example, a recent wave of Zelle fraud involves a scammer impersonating the bank, stating that the consumer's account was compromised, and telling the consumer to send the money to themselves by using Zelle to send the funds to their own cell phone. But behind the scenes, the scammer has linked the consumer's cell phone to the scammer's account. That is arguably a mistake by the scammer's bank, which linked the wrong phone number to that account. Yet banks refuse to help:

- "When Mr. Faunce called Wells Fargo to report the crime, the customer service representative told him, 'A lot of people are getting scammed on Zelle this way.' Getting ripped off for $500 was 'actually really good,' Mr. Faunce said the rep told him, because 'many people were getting hit for thousands of dollars.'"[58]

F. The Protecting Consumers From Payment Scams Act would protect consumers from fraud and errors in digital wallets and bank P2P services

The discussion draft of the Protecting Consumers From Payment Scams Act would address these gaps and ambiguities in the EFTA and Regulation E.[59] Some of these problems could also be addressed by rulemaking or guidance from the CFPB, though Congressional action would be faster and less subject to challenge.

---

[57] *See* Christopher Elliott, *A Venmo user sent $100 to the wrong person. Then the payment service froze his account*, Seattle Times (Nov. 2, 2020), *available at* https://www.seattletimes.com/life/travel/a-venmo-user-sent-100-to-the-wrong-person-then-the-payment-service-froze-his-account-travel-troubleshooter/.
[58] *See* Stacy Cowley, Lananh Nguyen, New York Times, "Fraud Is Flourishing on Zelle. The Banks Say It's Not Their Problem." (Mar. 6, 2022), https://www.nytimes.com/2022/03/06/business/payments-fraud-zelle-banks.html.
[59] https://financialservices.house.gov/uploadedfiles/bills-117pih-protectingconsumersfrompaym-u1.pdf.

The bill would:

- Protect consumers from liability when they are defrauded into initiating a transfer, and allowing the consumer's financial institution, after crediting the consumer for a fraudulent transfer, to be reimbursed by the financial institution that allowed the scammer to receive the fraudulent payment;
- Eliminate the exemption for bank wire transfers and electronic transfers authorized by telephone call, bringing those transfers within the EFTA and its protections against unauthorized transfers and errors;
- Clarify that error resolution duties apply if the consumer's account is frozen or closed or the consumer is otherwise unable to access their funds, unless access has been denied due to a court order or law enforcement, or the consumer obtained the funds through unlawful or fraudulent means;
- Clarify that the EFTA's error resolution procedures apply when the consumer makes a mistake, such as in amount or recipient;
- Closing other loopholes or ambiguities.

These protections are urgently needed, and should be adopted swiftly to protect consumers in today's digital wallets, bank P2P services, and the coming FedNow system.

II. Deposits Held in Digital Wallets Should Be Insured

Another profound safety threat to consumers who use nonbank digital wallets is the fact that their deposits may not be insured by the FDIC. Some banking apps operate in partnership with an insured depository institution, so that deposits are insured – at least once they get to the bank.[60] Traditional prepaid card accounts also typically hold their funds in a bank and provide pass-through deposit insurance.

But the largest digital wallet provider, PayPal, keeps most of consumers' funds on its own books where they are not insured. PayPal's 2021 10-K report reveals that $38.8 of customer balances are direct liabilities of PayPal and that that amount does not include separate funds held in third-party financial institutions where they are eligible for pass-through insurance.[61]

The fine print of PayPal's website discloses that "Cash funds held in a PayPal Balance account are not eligible for FDIC pass-through insurance coverage unless you have a PayPal Cash Card, or have enrolled in Direct Deposit, or have bought cryptocurrency."[62] But PayPal has refused to display the prominent short-form disclosure required under the CFPB's prepaid accounts rules,

---

[60] *See* FDIC, "Banking With Apps" (Nov. 2020), https://www.fdic.gov/resources/consumers/consumer-news/2020-11.html ("It is important to be aware that non-bank companies are never FDIC-insured. Even if they partner with FDIC-insured banks, funds you send to a non-bank company are not FDIC-insured unless and until the company deposits them in an FDIC-insured bank.").

[61] See PayPal Holdings, Inc., Form 10-K for the fiscal year ended Dec. 31, 2021 at 61, https://d18rn0p25nwr6d.cloudfront.net/CIK-0001633917/82fd6358-df11-4e57-af9d-a5c66d48fadb.pdf; *see also id.* at 71 ("We hold all customer balances, both in the U.S. and internationally, as direct claims against us which are reflected on our consolidated balance sheets as a liability classified as amounts due to customers. . . . We classify the assets underlying the customer balances as current based on their purpose and availability to fulfill our direct obligation under amounts due to customers. Customer funds for which PayPal is an agent and custodian on behalf of our customers are not reflected on our consolidated balance sheets. These funds include U.S. dollar funds which are deposited at one or more third-party financial institutions insured by the Federal Deposit Insurance Corporation ("FDIC") and are eligible for FDIC pass-through insurance (subject to applicable limits)."

[62] https://www.paypal.com/us/digital-wallet/send-receive-money/send-money.

which would require the simple statement: “Not FDIC insured.”[63] The CFPB’s prepaid account rules apply to digital wallets like PayPal’s that are capable of holding funds, but PayPal sued the CFPB and a lower court ruled for PayPal, though the case is on appeal.[64]

Similarly, Block’s 2021 Form 10-K discloses that it held $2.8 billion of "Customer funds" as current assets and also had $4 billion of "Customers payable" as current liabilities – that is, funds held on its own books. The “Customers payable” figure includes "the Company's liability for customer funds held *on deposit* in the Cash App."[65] Notably, those funds are described as being “on deposit,” even though funds are not insured unless the consumer holds a Cash Card.[66]

Holding consumer funds in this way exposes consumers to significant risk if PayPal or Block were to run into financial trouble. Though the companies hold investments against these funds and are covered by state money transmitter laws, those protections are not nearly the same as the guarantee provided by FDIC insurance.[67] If PayPal or Block were to enter into bankruptcy, even if consumers might ultimately get their money back, it could take a significant amount of time to sort out competing claims. In contrast, when banks fail, the FDIC normally ensures a smooth transition that provides consumers access to their funds the next day.

The ability to avoid paying for deposit insurance also gives these nonbank digital wallets an unfair edge over their competitors. Skimping on consumer protection is not an appropriate way to compete.

Most importantly, the law requires these deposits to be insured. As Prof. Emeritus Arthur E. Wilmarth, Jr., of George Washington University Law School has written:

> PayPal’s customer balances are functionally equivalent to bank checking deposits in view of its customers’ ability to withdraw their balances on demand and to use their balances to make payments to third parties. Courts could reasonably determine that PayPal is unlawfully engaged in “the business of receiving deposits” in violation of Section 21(a)(2) of the Glass–Steagall Act. Section 21(a)(2) prohibits every person other than a regulated U.S. depository institution from “engag[ing], to any extent whatsoever . . . in the business of receiving deposits subject to check or to repayment upon . . . request of the depositor.” In view of Section 21(a)(2)’s prohibition, PayPal—a nonbank money transmitter—is operating in very dangerous territory by accepting and holding tens of billions of dollars of customer funds that can be withdrawn on demand or transferred to third parties.[68]

---

[63] *See* CFPB, Preparing the short form disclosure for prepaid accounts at 6, https://files.consumerfinance.gov/f/documents/cfpb_prepaid_guide-to-short-form-disclosure.pdf.
[64] *See* PayPal, Inc. v. CFPB, 512 F.Supp.3d 1 (D.D.C 2020) (finding that the CFPB did not have the power to issue regulation requiring prepaid product providers to disclose specific information about fees using standard form); Pymnts.com, PayPal Wins Prepaid Card Regulation Lawsuit Against CFPB (Jan. 4, 2021), https://www.pymnts.com/legal/2021/paypal-wins-prepaid-card-regulation-lawsuit-against-cfpb/.
[65] Block, Inc., Form 10-K for the fiscal year ending Dec. 31, 2021 at 82, 100 (emphasis added), https://s29.q4cdn.com/628966176/files/doc_financials/2021/q4/13386837-50ba-466f-b8ff-81824f066c1e.pdf
[66] Cash App Terms of Service (Apr. 11, 2022), https://cash.app/legal/us/en-us/tos.
[67] Pew Charitable Trusts, Imperfect Protection: Using Money Transmitter Law to Insure Prepaid Cards (Mar. 2013), https://www.pewtrusts.org/~/media/legacy/uploadedfiles/pcs_assets/2013/pewprepaidmoneytransmitterpdf.pdf.
[68] Arthur E. Wilmarth, “The Pandemic Crisis Shows that the World Remains Trapped in a 'Global Doom Loop' of Financial Instability, Rising Debt Levels, and Escalating Bailouts” at 8, 40 Banking & Financial Services Policy Report No. 8 (August 2021), https://ssrn.com/abstract=3943328 (citing 12 U.S.C. § 378(a)(2) among other authorities).

Either the Justice Department or Congress should take action to ensure that consumer deposits held for banking purposes, which consumers reasonably expect to be safe, carry deposit insurance.[69]

III. Conclusion

Digital wallets provide consumers with many conveniences. But first and foremost, they must be safe. Congress, the CFPB and other agencies as appropriate must take action to ensure that consumers are not left unprotected when P2P providers let scammers into their systems and when they hold consumers funds.

With any questions, please contact Lauren Saunders, Associate Director of the National Consumer Law Center, at lsaunders@nclc.org.

Thank you for the opportunity to provide this statement for the record.

Yours very truly,

Consumer Federation of America
National Consumer Law Center (on behalf of its low-income clients)
National Consumers League
U.S. PIRG

[69] *See also* Arthur E. Wilmarth, "It's Time to Regulate Stablecoins as Deposits and Require Their Issuers to Be FDIC-Insured Banks" at 7-11, 41 Banking & Financial Services Policy Report No. 2 (Feb. 2022), https://ssrn.com/abstract=4000795 (discussing the Glass-Steagall Act's requirements for deposits).

STATEMENT FOR THE RECORD

Fabrice Coles
Senior Manager of Global Public Policy and Research
PayPal Inc.

BEFORE THE

United States House of Representatives
Committee on Financial Services
Task Force on Financial Technology

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

April 28, 2022

2:00 PM

Chair Lynch and Ranking Member Davidson, thank you for holding this important hearing to explore trends and developments in digital wallets. The hearing comes at a critical time for the country as financial services will be an important factor of Americans' recovery from the historic pandemic and its lingering effects, as well as our potential for improving and achieving universal financial health.

PayPal is a leading technology platform that enables digital payments and simplifies commerce experiences on behalf of merchants and consumers in 200 markets around the world. Our mission is to democratize financial services to ensure that everyone, regardless of background or economic standing, has access to affordable, convenient and secure products and services to take control of their financial lives, build resilience, and create capacity to achieve hopes and dreams. We aim to improve the financial health of individuals and to increase economic opportunity for entrepreneurs and businesses of all sizes around the world. We are aligned across the company around one central vision: to make the movement and management of money as simple, secure and affordable as possible.

We deliver our services responsibly by investing in compliance and risk management systems to empower and protect users, and to help ensure compliance with all applicable federal and state laws. PayPal's core payments services are regulated in the U.S. by the Consumer Financial Protection Bureau and at the state level as a licensed money transmitter. PayPal is a member of FinTech Industry Advisory Panel and related working groups established by U.S. state regulators (via the Conference of State Banking Supervisors), who have decades of experience regulating money services businesses, to ensure harmonization of existing state regulatory frameworks. Outside the U.S., our services are overseen by the relevant regulators in each of the jurisdictions in which we operate. Certain PayPal products are offered in partnership with banks which also brings regulatory oversight.

PayPal thrives because of the trust we have earned with our customers and the relationships built with regulators.

PayPal's Digital Wallet Offering

The PayPal app is an intelligent digital wallet that fosters a unique experience that is enhanced and tailored for each customer. The pandemic has transformed payments, and PayPal has been supporting our customers along this journey.

The PayPal app is a personalized set of services that offers customers the best place to manage their daily financial lives. As more and more people are using their smartphones to make purchases, receive payments, and manage their accounts, we offer individuals and businesses choices and flexibility when they send payments and receive payments. Whether sending money to friends and family through apps like PayPal, Venmo, and Xoom, engaging in e-commerce, or enabling people to support causes and charities they care about, our technology is providing more individuals and businesses with access to the global market and financial services tailored to their specific needs.

The PayPal wallet includes a personalized dashboard of a customer's account with PayPal; a wallet tab to manage payment instruments; and, a payments hub that includes send and receive money features, international remittances, and charitable/non-profit giving.

PayPal has been a leader in providing needed services to Americans during these trying times. PayPal and Venmo digital wallet users were able to cash their government-issued paper stimulus checks remotely, usually within minutes and free-of-charge. We also offered customers who received stimulus checks the ability to sign up for Direct Deposit to receive their funds faster.

The security and privacy of all our users and their information has always been a top company priority. Security has been front and center throughout the development of our digital wallet, as evidenced by the adoption of innovations such as tokenization technology, which reduces the number of entities that have access to sensitive financial data. PayPal has been a pioneer of tokenization technology, substituting a person's sensitive financial information with a series of non-sensitive numbers that confirm to the business that a payment is authentic, helping to minimize the likelihood and impact of data breaches as well as reduce fraud.

At PayPal, we regard fighting cybercrime as a strategic business priority, and we invest heavily in keeping our sites and services as safe and secure as possible. PayPal's philosophy on cybersecurity has a strong focus on customer data protection. Everything we do around security is focused on our commitment as the "secure way to pay and be paid." It is important to approach security holistically helping merchants keep their systems secure by analyzing data in real-time to understand behavior alongside static data to help verify identity and protect consumers. We also seek opportunities to assist law enforcement in the prevention and detection of financial crimes, including participation in industry – law enforcement alliances.

Digital wallet service providers can leverage key information from the mobile device to improve identification, authentication, and fraud reduction. PayPal is a founding member of the Fast IDentity Online (FIDO) Alliance whose mission is to find new methods of authentication that move away from passwords and towards biometrics (fingerprint, etc.). Moreover, should something go wrong with a purchase, *i.e.,* an item doesn't arrive, or what arrives is significantly different than what was described, then PayPal can cover customers under Purchase Protection for eligible purchases.

PayPal is Responsibly Democratizing Access to Financial Services

PayPal is proud of the leadership position it has established in responsible innovation in financial services. Our investments in innovation have helped usher in an era where our customers can safely exchange value quickly and easily all over the world. A key principle for our digital wallet offering is providing our customers with choices on how to exchange value across various well known and accepted retail payment options. Many of these options sit on top of long established and well-regulated payment systems like Automated Clearing House (ACH) or credit/debit networks.

With well-established payment systems serving as the underpinning of PayPal's digital payment services, PayPal maintains a robust control framework to ensure money moves safely and

securely. We regularly monitor activity on our platform, apply a robust Know Your Customer framework and maintain compliance with anti-money laundering requirements. PayPal has built a platform that responsibly leverages technology tools to enable seamless value transfer across several payment media while meeting our compliance obligations.

As this landscape continues to evolve, PayPal will continue to build its services with responsible innovation as a North Star. Our customers choose PayPal because we are a trusted platform and they feel safe leveraging our services as they pursue their options for digital commerce and payments. This trust can only be earned through a relentless focus on mitigating risks in our operating environment and protecting our customers from financial harms and as a result of this focus we strive to be thoughtful about how we design our products, policies and procedures.

We encourage continued public-private dialogue on these matters and look forward to continuing to engage with the Financial Technology Task Force and the broader House Financial Services Committee in important conversations related to the growth of the digital payments business in the United States. We are happy to share some initial thoughts with the Committee on the following issues and look forward to continued dialogue on the vital matters in the Committee's jurisdiction.

Stability and Data Security. PayPal invests heavily in compliance, risk management and information security to help ensure that our systems are reliable and operate soundly so that the services in our digital wallet can be offered without incident for our customers or the broader payments system. PayPal's operations, capital and liquidity are regulated by dozens of state financial regulators as a part of the money transmitter licensing requirements.

Customer Liquidity. PayPal is a digital wallet provider, not a bank. It does not accept deposits. Customers typically add value to a PayPal account from an existing bank account or card. For PayPal Balance account holders, PayPal also permits consumers to add value to their accounts via cash uploads at thousands of participating retailers. PayPal Savings, provided by an FDIC insured bank partner, is a savings account available in the digital wallet for PayPal Balance account holders.

Privacy. PayPal deeply values the trust of its customers and takes their privacy seriously. The firm is subject to the Gramm Leach Bliley Act (GLBA) and Reg P covering consumer privacy.

Financial Crime. PayPal is a registered Money Services Business with the US Treasury Department and is therefore required by the Financial Crimes Enforcement Network (FinCEN) to maintain a compliance program dedicated to anti-money laundering. We deploy rigorous know-your-customer (KYC) requirements, screening, and other sophisticated tools to mitigate financial crime risks.

Community Investment. PayPal invests in and supports community organizations across our global footprint, especially in businesses and non-profits that invest in underserved communities. For example, in addition to facilitating fundraising and disaster relief with

charitable organizations, PayPal has committed $535 million dollars to help support work in narrowing the racial wealth gap and empower equity.

Conclusion

Fueled by a fundamental belief that having access to financial services creates opportunity, PayPal is committed to democratizing financial services and empowering people and businesses to join and thrive in the global economy. We believe that individuals, families, small businesses and communities will benefit from the continued melding of digital wallet technology and payments, as well as increased competition.

Thank you again for the opportunity to provide a statement for the record to the Task Force on this important and timely topic.