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).