Testimony of

John Breyault

Vice President of Public Policy, Telecommunications, and Fraud

National Consumers League

on

"Protecting Consumers from Financial Fraud and Scams in the Pandemic Recovery Economy"

Before the

United States Senate

Committee on Banking, Housing, and Urban Affairs

Subcommittee on Financial Institutions and Consumer Protection

August 3, 2021

Summary

The COVID-19 pandemic has been a boom time for scammers and a nightmare for their victims. By almost any measure, rates of fraud related to the pandemic have mushroomed. In 2020, the Federal Trade Commission received more fraud complaints than at any time in its 106-year history. The House Select Subcommittee on the Coronavirus Crisis estimates that potential fraud involving the Small Business Administration's Paycheck Protection Program ("PPP") and Economic Injury Disaster Loan ("EIDL") programs could cost taxpayers $84 billion. The impact of this fraud has fallen disproportionately on historically marginalized communities, already suffering from high rates of COVID-related illnesses, deaths, and economic hardship.

We are pleased to contribute to the subcommittee's examination of the role that insecure peer-to-peer ("P2P") payment platforms are playing in the transfer of funds from fraud victims to scammers during the pandemic. Unfortunately, the same features that are fueling these services' explosive growth – low cost, nearly instantaneous payments made via a mobile app – have made P2P an increasingly popular payment method for scammers. Analysts estimate that fraud rates on these platforms are three to four times higher than for traditional payment methods such as debit and credit cards.

The lack of consumer protections for victims is a significant reason why fraud rates are so high. Scammers are unlikely to abandon P2P platforms as long as they can be used to easily obtain fraudulent payments. To address this, we recommend that Congress consider extending existing limited liability protections for debit and credit card transactions to cover fraudulently induced payments, requiring more stringent investigations of potentially fraudulent transactions, pushing regulators to enforce error resolution responsibilities for consumer errors and fraudulently induced payments, and mandating more responsive customer service by P2P platforms.

Introduction

The National Consumers League appreciates the opportunity to provide the subcommittee with our views on protecting consumers from financial fraud and scams as America begins to emerge from the COVID-19 pandemic.

Founded in 1899, the National Consumers League ("NCL") is the nation's pioneering consumer and worker advocacy organization. Our non-profit mission is to advocate on behalf of consumers and workers in the United States and abroad.[1] For more than twenty years, NCL has worked, via our Fraud.org campaign, to educate consumers about the warning signs of fraud and promote public policies that protect the American public from scams of all kinds.

The COVID-19 Pandemic Has Been A Perfect Storm For Fraudsters

The last sixteen months have been boom times for scammers and a nightmare for their victims. To put this in context, in 2020 the Federal Trade Commission ("FTC") received 4.72 million complaints from consumers, a 45.7% increase over 2019 and by far the largest year-over-year increase in the FTC's history.[2] The median loss reported by victims of these scams was $374, though many victims lost far more. A consumer who contacted NCL's Fraud.org campaign lost $15,000 to a scammer.[3] What is clear is that even these sobering numbers are only the tip of a gigantic iceberg when it comes to COVID-linked fraud.

For example, the Department of Labor recently estimated that one type of fraud alone – unemployment insurance fraud – will have cost taxpayers more than $87

[1] For more information, visit www.nclnet.org.
[2] Federal Trade Commission. *Consumer Sentinel Data Book 2020*. February 2021. Pg. 6. Online: https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf
[3] Fraud.org. "Cash App scams on the rise," June 1, 2021. Online: https://fraud.org/cash_app_alert/

billion over the course of the pandemic.[4] Other estimates have put the amount of unemployment fraud during the pandemic as high as $400 billion.[5] Fraudsters are having a heyday. One Bronx man received $1.5 million in ten months, a California real estate broker stole more than $500,000 over 6 months, and a Nigerian government official was recently accused of fraudulently obtaining over $350,000 in less than six weeks.[6] Even high-profile politicians are not immune. The personal information of Senator Diane Feinstein[7] and Ohio Governor Mike DeWine[8] was reportedly used by unemployment insurance fraudsters to try and improperly obtain benefits.

The statistics are equally sobering for fraud involving other pandemic relief programs. A recent analysis by the House of Representatives' Select Subcommittee on the Coronavirus Crisis identified nearly $84 billion in potential fraud involving the Small Business Administration's Paycheck Protection Program ("PPP") and Economic Injury Disaster Loan ("EIDL") programs.[9]

---

[4] United States Department of Labor Office of Inspector General. "DOL-OIG Oversight of the Unemployment Insurance Program," June 10, 2021. Online: https://www.oig.dol.gov/doloiguioversightwork.htm

[5] Salmon, Felix. "Half of the pandemic's unemployment money may have been stolen," *Axios*. June 10, 2021. Online: https://www.axios.com/pandemic-unemployment-fraud-benefits-stolen-a937ad9d-0973-4aad-814f-4ca47b72f67f.html

[6] Podkul, Cezary. "How Unemployment Insurance Fraud Exploded During the Pandemic," *ProPublica.* July 26, 2021. Online: https://www.propublica.org/article/how-unemployment-insurance-fraud-exploded-during-the-pandemic

[7] White, Jeremy. "Californian allegedly obtained UI benefits using Feinstein's identity," POLITICO. December 17, 2020. Online: https://www.politico.com/states/california/story/2020/12/17/californian-allegedly-obtained-ui-benefits-using-feinsteins-identity-1348423

[8] Bischoff, Laura. "Unemployment fraud so 'widespread' it even happened to DeWine and Husted," *Dayton Daily News*. January 19, 2021. Online: https://daytondailynews.com/local/unemployment-fraud-so-widespread-it-even-happened-to-dewine-and-husted/XRDFXUC7EFHKVD2C54SEJGFCCQ/

[9] House Select Subcommittee on the Coronavirus Crisis. "Lowering the Guardrails: How the Trump Administration Failed to Prevent Billions in Pandemic Small Business Fraud," March 25, 2021. Online: https://coronavirus.house.gov/sites/democrats.coronavirus.house.gov/files/2020-03-25%20Staff%20Memo%20-%20Small%20Business%20Fraud.pdf

The variety of scams linked to COVID-19 is staggering. Fraudsters have run advance fee scams targeting consumers' stimulus checks.[10] They have committed identity fraud linked to the sharing of COVID-19 vaccination cards online.[11] Imposter scams have preyed on consumers' fears about Federal Deposit Insurance Corporation-backed bank accounts.[12] Scammers even taken advantage of grieving families by targeting the Federal Emergency Management Agency's COVID-19 Funeral Assistance Program.[13]

The Department of Justice and other enforcement agencies have done yeoman's work to try and crack down on this wave of criminality, particularly scams targeting taxpayer-funded COVID-19 relief programs.[14] Unfortunately, given the scale of fraud linked to the pandemic, these efforts are likely to be little more than temporary setbacks for the armies of sophisticated and well-organized criminal rings.

Many factors have contributed to the historic increase in fraud during the pandemic. Rampant misinformation and disinformation about the virus have been fertile ground for scammers peddling all manner of COVID-prevention pills, testing kits, and treatments. Unprecedented economic distress has created ample opportunities for scammers to run imposter schemes threatening dire consequences if payments aren't made. Scammers can easily contact victims over the phone, text message, email or over the Web, putting millions of potential victims at their fingertips. These transactions happen with speed and anonymity through gift cards, peer-to-peer

[10] Leonhardt, Megan. "5 common stimulus check scams experts are warning consumers to watch for," CNBC.com. December 29, 2020. Online: https://www.cnbc.com/2020/12/29/stimulus-check-scams-here-are-red-flags-to-watch-for.html

[11] Gressin, Seena. "Social media is no place for COVID-19 vaccination cards," Federal Trade Commission. February 5, 2021. Online: https://www.consumer.ftc.gov/blog/2021/02/social-media-no-place-covid-19-vaccination-cards

[12] Federal Deposit Insurance Corporation. "FDIC: Insured Bank Deposits are Safe: Beware of Potential Scams Using the Agency's Name." Press Release. March 18, 2020. Online: https://www.fdic.gov/news/press-releases/2020/pr20032.html

[13] Gressin, Seena. "Scammers target loved ones of COVID-19 victims." MilitaryConsumer.gov. April 20, 2021. Online: https://www.militaryconsumer.gov/blog/scammers-target-loved-ones-covid-19-victims

[14] United States Department of Justice. "Justice Department Takes Action Against COVID-19 Fraud." Press release. March 26, 2021. Online: https://www.justice.gov/opa/pr/justice-department-takes-action-against-covid-19-fraud

("P2P") payment apps, cryptocurrencies and other money transfer services. Cashing out is easy and relatively risk-free for the criminals.

Taken together, these factors have created a perfect storm of fraud during the pandemic.

The Impact of Fraud Linked to COVID-19 Has Fallen Disproportionately On Marginalized Communities

Consumers' vulnerability to fraud increases during times of economic uncertainty. The COVID-19 pandemic has been no exception. High unemployment, the threat of eviction, and social isolation brought on by social distancing measures have all contributed to high rates of fraud.

While fraud affects consumers of all races, ages and income levels, consumers from historically marginalized communities have been at particular risk of scams. According to a 2017 FTC survey, 19.2% of African Americans and 17.3% of Hispanic consumers reported being a victim of fraud compared to 15.9 % of consumers overall and 14.9% of non-Hispanic Whites.[15] The same survey found that 20.4% of consumers who have experienced a serious negative life event (e.g. death of a family member or close friend, a serious injury or illness in the family, or the loss of a job) reported being victims of fraud, compared to 13.1% of consumers who had not experienced such an event.[16]

Specific data on the intersection of COVID-19 fraud and minorities is lacking. However, given what we know about the vulnerability of consumers of color to

[15] Anderson, Keith. *Mass-Market Consumer Fraud in the United States: A 2017 Update.* (Staff Report of the Bureau of Economics, Federal Trade Commission.) Table 11. October 2019. Online: https://www.ftc.gov/system/files/documents/reports/mass-market-consumer-fraud-united-states-2017-update/p105502massmarketconsumerfraud2017report.pdf
[16] *Ibid.* Pg. 106.

fraud and the high toll that COVID-19 has taken on their communities in terms of deaths, illnesses, and economic harm,[17] we can conclude that fraud linked to the pandemic is taking a similarly disproportionate toll on historically marginalized consumers.

Anecdotal evidence supports this conclusion. This spring, the FTC and the state of Arkansas sued the operators of a "blessing loom" pyramid scheme that allegedly targeted African Americans struggling financially during the pandemic. According to the FTC, the scammers behind the scheme defrauded thousands of consumers of tens of millions of dollars by promising investment returns as high as 800%.[18] The National Caucus and Center on Black Aging has also reported an increase in fraud cases targeting cash-strapped or unemployed older African Americans since the pandemic began.[19]

Scammers Are Exploiting a Lack of Protections for Payments Made Via Peer-to-Peer Services

The ultimate goal for fraudsters is stealing money. This can take the form of direct payments from the victims to the scammers or stealing information that can then be used to obtain money through identity fraud or other schemes. Scammers routinely take advantage of new financial technologies to facilitate the transfer of funds. While no financial institution wants to be used as a vehicle for crime, there is often tension

[17] Zamarripa, Ryan and Roque, Lorena. "Latinos Face Disproportionate Health and Economic Impacts From COVID-19." Center for American Progress. March 5, 2021. Online: https://www.americanprogress.org/issues/economy/reports/2021/03/05/496733/latinos-face-disproportionate-health-economic-impacts-covid-19/

[18] Federal Trade Commission. "FTC and the State of Arkansas Charge Operators of 'Blessing Loom' With Running an Illegal Pyramid Scheme." Press release. June 17, 2021. Online: https://www.ftc.gov/news-events/press-releases/2021/06/ftc-state-arkansas-charge-operators-blessing-loom-running-illegal

[19] NAACP. "Elder Abuse: Another COVID-19 Evil," March 1, 2021. Online: https://naacp.org/articles/elder-abuse-another-covid-19-evil

between businesses' desire to secure a particular payment vector from fraud while still allowing for legitimate transactions to be processed quickly.

This tension is clear when it comes to the rapid growth of P2P payment platforms such as PayPal's Friends & Family and Venmo services, Square's Cash App, and Zelle, which is owned by a consortium of major banks. These services have attracted tens millions of users by allowing for free or very low-cost payments to be sent between consumers or from consumers to businesses.[20] Even before the pandemic, roughly 4 in 5 Americans (79%) has used mobile payment apps, by one estimate.[21] Social distancing regulations put in place during the pandemic have supercharged consumers' embrace of these services, with the volume of payments expected to grow by roughly 37% in 2021.[22] The explosive growth of these services is not expected to end any time soon. By 2023, it is estimated that more than $1 trillion will be transacted via P2P platforms.[23]

Unfortunately, the same factors that are fueling the rapid growth of P2P payment platforms during the pandemic – low-cost, nearly instantaneous payments made via a mobile app – have made P2P a payment method of choice for scammers. In 2020, the FTC received nearly 62,000 complaints from consumers who sent money to fraudsters via payment apps or similar services, with a total reported loss of $87 million.[24] Consumer complaints to the Consumer Financial Protection Bureau ("CFPB" or "Bureau") tell a similar story. A recent MASSPIRG Education Fund

---

[20] Kunst, Alexander. *Statista Global Consumer Survey*. November 19, 2020. Online: https://www.statista.com/forecasts/997123/peer-to-peer-payments-in-the-us

[21] El Issa. "Most Americans Go Mobile With Payment Apps – Here's How They Roll," NerdWallet.com. February 26, 2020. Online: https://www.nerdwallet.com/article/banking/mobile-payment-app-survey

[22] Ho, Justin. "P2P payment apps are booming, thanks to the pandemic," Marketplace.org. March 15, 2021. Online: https://www.marketplace.org/2021/03/15/p2p-payment-apps-are-booming-thanks-to-the-pandemic/

[23] Kats, Rimma. "In 2023, more than $1 trillion will transact via mobile P2P apps," *Insider Intelligence*. April 19, 2021. Online: https://www.emarketer.com/content/breaking-down-mobile-p2p-payments-biggest-players

[24] Federal Trade Commission. *Consumer Sentinel Network Data Book 2020.* February 2021. Pg. 11. Online: https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf

analysis found that more than 5,200 complaints about mobile or digital wallets were filed with CFPB over the 12-month period preceding April 2021. Three companies – PayPal (which owns Venmo), Square (which owns Cash App), and Coinbase (a platform for buying and selling cryptocurrency) – accounted for more than two-thirds of all digital wallet complaints to the Bureau through April 2021.[25] The Better Business Bureau has reported a similar increase in complaints involving P2P services.[26]

A complaint NCL received recently from a consumer in Pennsylvania is typical of the experience for far too many consumers who are induced to send money to fraudsters via P2P payment apps. In the process of trying to activate her Cash Card debit card for Square's Cash App service, the consumer's wife was directed to a phishing website where she inadvertently gave a scammer access to her Cash App account. The fraudsters quickly drained more than $5,000 from the consumer's account. When the consumer contacted his bank and Cash App to address the fraud he was told there was nothing that could be done because he his wife had given her permission for the transaction to the scammer.

Another consumer from Massachusetts sent us a similar story last year. She thought she had booked a vacation rental in Provincetown and she was instructed by the "owner" of the property to send a $1,150 deposit via PayPal. When she arrived at the address on the listing, she found that no such property existed. "The neighbor told me he'd heard of many such scams in Provincetown," she wrote.[27] She contacted PayPal twice to dispute the transaction, but was told that there was nothing that could be done to get her money back.

---

[25] Mierzwinski, Ed *et al*. *Virtual Wallets, Real Complaints*. MASSPIRG Education Fund. June 2021. Pg. 2. Online: https://masspirg.org/sites/pirg/files/reports/MA_wallets.pdf

[26] Zamost, Scott. "Criminals launder coronavirus relief money, exploit victims through popular apps," CNBC.com. November 18, 2020. Online: https://www.cnbc.com/2020/11/18/criminals-launder-coronavirus-relief-money-exploit-victims-through-popular-apps.html

[27] *See, e.g.* Martin, Sean. "Vacationers continue to be fooled by rental scams," *Provincetown Banner*. August 15, 2019. Online: https://provincetown.wickedlocal.com/news/20190815/vacationers-continue-to-be-fooled-by-rental-scams

P2P services are aware that fraudsters use their services to obtain funds from their victims. An NCL review found that all of the major P2P platforms make some effort to educate their users about how to avoid scams. However, voluntary disclosures or consumer education alone are not terribly effective by themselves. Despite the platforms' efforts to educate users about the risks of sending money via P2P platforms, more than half of consumers surveyed by AARP incorrectly assumed that their payments would be protected if there is an error or fraud associated with the transaction.[28]

While P2P services do employ technological measures to stop fraudulent transactions, there is a business incentive not to introduce too many security roadblocks in the payment process. This is because P2P payment platforms, and their sky-high valuations,[29] [30] are dependent on maintaining large transaction volumes. P2P platforms' desire to reduce "friction" in the payments experience is in direct tension the need to prevent fraud.[31] Yet if these platforms are making the decision to skew their services towards speed and convenience at the expense of safety and protection, they must take responsibility for those choices.

What is clear is that existing efforts to secure P2P payments are falling far short of what is needed. Major P2P platforms operators like Square, PayPal and Zelle do not publicly disclose their fraud rates. They should be required to do so. Analysts estimate that fraud rates on these platforms are three to four times higher than

---

[28] AARP. "AARP Survey Finds Majority of Americans Using Payment Apps Unaware of Danger Posed by Scammers." Press release. May 12, 2020. Online: https://press.aarp.org/2020-5-12-AARP-Survey-Finds-Majority-of-Americans-Using-Payment-Apps-Unaware-of-Danger-Posed-by-Scammers

[29] Hale, Kori. "Hip-Hop's Role in Square's $40 Billion Cash App Business Success," *Forbes*. September 22, 2020, Online: https://www.forbes.com/sites/korihale/2020/09/22/hip-hops-role-in-squares-40-billion-cash-app-business-success/?sh=10d7f8ee7489

[30] Rudegeair, Peter. "Cash App's Surge During Covid-19 Pandemic Fuels Square Stock," *Wall Street Journal*. September 2, 2020. Online: https://www.wsj.com/articles/cash-apps-surge-during-covid-19-pandemic-fuels-square-stock-11599039003

[31] Doyle, Ciaran. "Removing friction & fraud from P2P payments," *IBM RegTech Innovations*. December 6, 2018. Online: https://www.ibm.com/blogs/regtech/removing-friction-and-fraud-from-p2p-payments/

traditional payment methods such as debit and credit cards.[32] Javelin Strategy & Research recently found that P2P services saw a 733% increase in fraud from 2016 to 2019.[33] The popularity of P2P payments during the pandemic is also evident from conversations among fraudsters themselves on the Dark Web. In August 2020 alone, analysts noted that Cash App was mentioned more than 10,500 times, an increase of 450% from the previous year. Listings mentioning Venmo and Zelle increased by around 50% in the same period.[34]

While no financial service is immune from fraud, protections for consumers who lose money to scammers on P2P apps are sorely lacking. When scammers obtain a consumer's bank account information and use it to initiate a preauthorized payment through the ACH system, or obtain debit card information and use it to initiate payment for fraudulent purchases, the consumer typically has limited liability for such transactions, thanks to the federal Electronic Funds Transfer Act ("EFTA"), implemented through the Federal Reserve's Regulation E.[35] Similar consumer protections exist for fraudulent credit card transactions exist under the Fair Credit Billing Act ("FCBA").[36] Thanks to these measures, consumers are protected, and credit and debit card issuers and participants in the ACH system have strong incentives to implement stringent anti-fraud countermeasures. The benefits to consumers of these regulatory incentives is clear. Today, it is not uncommon for a credit card holder whose account has been compromised to be notified by her bank before she even notices a fraudulent charge on her statement.

---

[32] Popper, Nathaniel. "When Your Last $166 Vanishes: 'Fast Fraud' Surges on Payment Apps," *New York Times*. October 11, 2020. Online: https://www.nytimes.com/2020/10/11/technology/fraud-payment-apps.html

[33] Javelin Strategy & Research. "Identity Fraud Losses Increase 15 Percent as Consumer Out-of-Pocket Costs More Than Double, According to 2020 Identity Fraud Report." Press release. May 13, 2020. Online: https://www.javelinstrategy.com/press-release/identity-fraud-losses-increase-15-percent-consumer-out-pocket-costs-more-double

[34] [34] Popper, Nathaniel. "When Your Last $166 Vanishes: 'Fast Fraud' Surges on Payment Apps," *New York Times*. October 11, 2020. Online: https://www.nytimes.com/2020/10/11/technology/fraud-payment-apps.html

[35] Federal Deposit Insurance Corporation. "Laws and Regulations: Electronic Funds Transfer Act." February 2019. Online: https://www.fdic.gov/news/financial-institution-letters/2019/fil19009b.pdf

[36] 15 U.S.C. 1666-1666j

Unfortunately, while P2P platforms are covered by the EFTA, victims of fraud committed via P2P platforms are often unable to take advantage of the protections afforded. A big reason for this is a loophole in the EFTA that excludes payments initiated by the consumer from the protection for unauthorized charges (also known as "fraud in the inducement" or "victim-assisted fraud").[37] This allows P2P services and banks to avoid liability for payments sent from consumers to scammers, even when such payments are induced by fraud.[38]

The end result of the loophole for fraudulently induced payments made via P2P platforms is that the liability risk for fraud is transferred from P2P platforms and banks to consumers themselves. Yet it is the platforms that have designed systems that encourage this type of fraud and who set the level of fraud they are willing to tolerate. Moreover, institutions are far more able to handle the costs of protecting consumers from small amounts of fraud in the system, whereas a single instance of fraud can be devastating to a consumer. Unfortunately, the only recourse for many victims of fraud committed via P2P platforms is to throw themselves at the mercy of the banks or P2P platforms and beg to be made whole. Unfortunately, thanks to the lack of legal protections, it is far too easy for the banks and P2P platforms to simply tell fraud victims that they are out of luck.

Indeed, another problem is that most financial institutions are taking an unduly narrow view of their error resolution responsibilities under the EFTA. When consumers call to complain about a fraudulently induced payment, or about a mistake such as entering the wrong amount or wrong cell phone number for the recipient, many institutions are refusing to treat that as an error and refusing to investigate or to try to resolve it. Yet there is nothing in the EFTA or Regulation E that excludes consumer errors from the definition of "error." Even if a consumer

[37] Cornell Law School Legal Information Institute. "Fraud in the Inducement." June 2020. Online: https://www.law.cornell.edu/wex/fraud_in_the_inducement#:~:text=Fraud%20in%20the%20inducement%20occurs,damages%20or%20terminate%20the%20contract

[38] Mierzwinski, Ed *et al*. *Virtual Wallets, Real Complaints*. MASSPIRG Education Fund. June 2021. Pg. 9. Online: https://masspirg.org/sites/pirg/files/reports/MA_wallets.pdf

might ultimately be liable for a payment because it was initiated by the consumer and thus is not "unauthorized," that does not mean that institutions do not have a duty to investigate and try to resolve the matter. A refusal to take these fraud reports and to pass them on to the receiving institution also deprives that institution that holds the scammer's account (or that of a money mule who themselves may be a victim of fraud) of the information needed to put a hold on the funds or shut down that account to prevent further fraud.

Difficulty in obtaining appropriate customer service is especially acute with app-based services that rely on automated communications and do not make live customer service available or adequately staff customer service lines. Problems that consumers have experienced with neo-bank accounts like Chime show the importance of making human beings available to address problems when things go wrong.[39]

The Federal Reserve should ensure that FedNow is safe for consumers before the system is launched.

The Federal Reserve Board ("FRB") is in the middle of building a new faster payment system called FedNow, which will be an alternative to Zelle and other private systems.[40] The FRB has recently proposed one set of rules governing the system.[41]

[39] Kessler, Carson. "A Banking App Has Been Suddenly Closing Accounts, Sometimes Not Returning Customers' Money." *ProPublica*. July 6, 2021. Online: https://www.propublica.org/article/chime?utm_source=sailthru&utm_medium=email&utm_campaign=dailynewsletter&utm_content=feature

[40] Tahyar, Margaret *et al*. "FedNow: The Federal Reserve's Planned Instant Payments Service," *Harvard Law School Forum on Corporate Governance.* August 31, 2020. Online: https://corpgov.law.harvard.edu/2020/08/31/fednow-the-federal-reserves-planned-instant-payments-service/

[41] FRS-2021-0214-0001. Online: https://www.regulations.gov/document/FRS-2021-0214-0001

We see the value in the FRB's decision to build a real time payment system. It is imperative, however, that the inadequacies in consumer protection with regards to fraudulent P2P payments not be exacerbated as the FRB continues development of its FedNow service.[42] The rules proposed to date do not address the problems discussed in these comments.

As a public body, the FRB has an especially great responsibility to make sure that a system it designs and runs is safe. Protections in the FedNow system can be a model for other P2P systems. Congress has a critical role to play by insisting that the FRB meets this challenge. Now, during its design phase and before it is deployed to the public, these challenges must be addressed.

New Protections Are Needed to Protect Consumers From Fraud And Errors On P2P Payment Platforms

The lack of consumer protections for users of P2P payment platforms must not be ignored. It is clear from their explosive growth that P2P payment apps are here to stay. It is equally clear that absent regulatory incentives, effective self-regulation by the P2P services will be stymied in the name of protecting transaction volume growth. NCL has spoken with P2P platforms and urged them to offer far more robust fraud protection, but so far we have seen little improvement. The P2P services will continue to rely on marginally effective warnings and disclosures to consumers – an old-fashioned tactic – rather than embracing their responsibility to design systems for safety and using modern artificial intelligence, machine learning, data analytics and other methods to prevent and remedy fraud.

[42] Letter from Americans for Financial Reform Education Fund *et al* to Board of Governors of the Federal Reserve System. November 7, 2019. Online: https://www.nclc.org/images/pdf/cons-protection/coalition-letter-interbank-settlements.pdf

To ensure that P2P platforms are secure for their users and do not continue to be powerful tools for fraudsters, action by Congress is urgently needed.

Specifically, we urge Congress to:

- Enact legislation to expand the definition of "unauthorized electronic fund transfer" in the Electronic Funds Transfer Act to cover fraudulently induced payments, with ultimate liability resting with the institution that received the fraudulent payment;

- Push regulators to require P2P platforms to investigate errors and fraud, even in cases where the consumer sent a payment erroneously or as a result of fraud in the inducement;

- Urge bank regulators to emphasize fraud prevention and remediation as part of financial institutions' know-your-customer duties;

- Enact legislation to require P2P platforms to prominently display warning about fraudulent use of P2P payments and how to avoid scams;

- Require P2P platforms to provide and prominently display a customer service telephone line and respond to customer service inquiries in a timely manner; and.[43]

- Insist that the Federal Reserve promulgate rules for the design of the FedNow payments service that prioritize safety and security of payments.

[43] Note: The California legislature is currently considering AB-1320, which contains similar requirements. Online: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202120220AB1320

Conclusion

Chairman Warnock, Ranking Member Tillis and the members of the subcommittee, we thank you for your continuing work to protect consumers and for holding this hearing. On behalf of the National Consumers League, thank you for including the consumer perspective as you consider these important issues.