65 Consumer, Civil Rights, Faith, Legal Services and Community Groups

December 21, 2021

Submitted to Regulations.gov

Director Rohit Chopra
Bureau of Consumer Financial Protection
1700 G Street NW
Washington, DC 20552

Re: Big Tech Payment Platforms, Docket No. CFPB-2021-0017

Dear Director Chopra,

The 65 undersigned consumer, civil rights, faith, legal services and community groups submit these comments in response to the Consumer Financial Protection Bureau's (CFPB) inquiry into certain business practices of six large technology companies operating payments systems in the United States. In these comments, we would like to focus on consumer protections in those payment systems, and in particular the lack of protection against consumer errors and fraud. We also discuss the application of existing federal data governance laws. These comments will not address other privacy issues, but we agree with other commenters that any data collected through payment systems should be used only with consumer permission and in ways that they would expect.

Scams and errors can have a particularly harsh impact on low-income families and communities of color. 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 lack of protection in p2p systems plagues not only the payment systems of large technology companies but also new or proposed faster p2p payment systems that operate through banks and credit unions. Accordingly, we urge the CFPB to:

- 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.

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

- Clarify application of existing federal data governance laws including the Gramm-Leach-Bliley Act (GLBA) and possibly the Fair Credit Reporting Act (FCRA).

As consumer, small business, civil rights, community and legal service groups described at greater length in comments submitted three months ago to the FRB, the existing p2p payment systems of large technology companies and financial institutions simply are not safe for consumers to use.[1] Scams often take the last dollar from those least able to afford it, and often target older adults, immigrants and other communities of color.[2] 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. Fast 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.

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 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 the most important thing the CFPB can do, 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

---

[1] *See* Letter from 43 consumer, small business, civil rights, community and legal service groups to Board of Governors of the Federal Reserve System 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/FedNowCoalitionComments; Comments of National Consumer Law Center, National Community Reinvestment Coalition, 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.

[2] 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.

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 primary response of payment system providers 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 their 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.

Accordingly, we have five requests.

1. **The CFPB should make clear that the existing obligation under the EFTA to investigate and resolve errors applies in the case of consumer errors in p2p systems.** There are no limitations in the definition of "error" that would eliminate errors committed by consumers.[3] 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. **The CFPB should ensure that consumers using p2p services have protection from scammers, using the Bureau's EFTA rulemaking authority to define additional "errors."[4]** While payments that consumers are fraudulently induced to send fall outside of the definition of "unauthorized charge,"[5] fraudulently induced payments can still be

[3] 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.
[4] 15 U.S.C. § 1693f(f)(7).
[5] *See* 15 U.S.C. §1693a(12).

considered an error triggering a duty to investigate and resolve the error.[6] A payment that was sent to an imposter or under other situations involving fraud can and should be deemed an error.

3. **Most urgently, the CFPB must work with the FRB to improve the proposed rules governing the FedNow system to add in protection against consumer errors and fraud.** The FedNow system should not be launched unless and until consumers (and small businesses) are protected from fraud and errors. Consumer protection issues cannot be ignored in the FedNow rules and cannot wait for EFTA rules covering the entire market. We have an opportunity now for FedNow to be a model for how other p2p systems can and should operate, and the CFPB and FRB should work together to seize that opportunity.

4. **The CFPB should clarify the rules and protections when accounts are frozen**. If a financial institution freezes an account because it spots red flags of fraudulent use or identity theft, it is not clear how long the freeze may last or what rights consumers have if they believe their account was wrongfully frozen. Our general view is that consumers 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: Unless law enforcement requires a different result, the institution should have 10 days to resolve whether any funds in the account should be unfrozen or whether the funds should be returned to the sender (or held for distribution to victims). But the topic deserves more consideration, as we recognize that the correct result requires balancing the importance of stopping fraudulent use with the rights of consumers whose accounts are incorrectly frozen.

5**. With respect to data sharing issues, we urge the CFPB to make clear the application of existing federal data governance laws, including GLBA and the FCRA.** A p2p payment system is most definitely a "financial institution" under GLBA since payment processing is a "financial activit[y] as described in" the Bank Holding Act.[7] Thus, any sharing of information with third parties is subject to the privacy notice requirements of 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 be a furnisher under 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-

[6] For example, the definition of "unauthorized transfer" also excludes a transfer by the financial institution or its employee, 12 C.F.R. § 1005.2(m)(3), but a "consumer has no liability for erroneous or fraudulent transfers initiated by an employee of a financial institution," Official Interpretation of Regulation E 2(m)-1

[7] 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).

covered purpose. And if consumer report information is shared internally between affiliated companies, the affiliate marketing provisions of the FCRA are implicated.[8]

Thank you for considering these comments.

A New Leaf, MesaCAN
Alaska PIRG
Americans for Financial Reform Education Fund
Arizona PIRG
Arkansans Against Abusive Payday Lending
Atlanta Legal Aid Society, Inc.
California PIRG
California Reinvestment Coalition
Center for Economic Integrity
Center for LGBTQ Economic Advancement & Research (CLEAR)
Colorado PIRG
Community Action Human Resources Agency (CAHRA)
Congregation of Our Lady of Charity of the Good Shepherd, U.S. Provinces
Consumer Action
Consumer Federation of America
Consumer Reports
Consumers for Auto Reliability and Safety
Georgia Watch
Greater Boston Legal Services
Housing and Economic Rights Advocates
Illinois PIRG
Legal Action Chicago
Legal Aid Justice Center
Legal Services of New Jersey
Maryland Consumer Rights Coalition
Maryland PIRG
Missouri Faith Voices
NAACP
National Advocacy Center of the Sisters of the Good Shepherd
National Association of Consumer Advocates
National Community Action Partnership
National Community Action Partnership
National Consumers League
National Council on Independent Living
National Employment Law Project
National Fair Housing Alliance
New Jersey Appleseed Public Interest Law Center

[8] 15 U.S.C. §§ 1681a(d)(2)(A)(iii), 1681s-3.

New Jersey Citizen Action
New Jersey Citizen Action
New Jersey Institute for Social Justice
New Jersey PIRG
North Carolina PIRG
Oregon PIRG
Pennsylvania PIRG
Prof. Cathy Mansfield, Case Western Reserve University Law School
Prosperity Works
Public Citizen
Public Good Law Center
Public Justice Center
RAISE Texas
RESULTS
RESULTS DC/MD
SC Appleseed Legal Justice Center
Texas Appleseed
Texas PIRG
Tzedek DC
U.S. PIRG
University of Iowa Law and Policy in Action Clinic
Virginia Citizens Consumer Council
Virginia Organizing
Virginia Poverty Law Center
Washington PIRG
Wildfire: Igniting Community Action to End Poverty in Arizona
Wisconsin PIRG
Woodstock Institute