Request for Information on Bank-Fintech Arrangements Involving Banking Products and Services Distributed to Consumers and Businesses

Comments on the Risks of Arrangements Impacting Payments and Deposit Accounts

to the

Office of the Comptroller of the Currency (OCC)
Regarding
Docket ID OCC-2024-0014

Board of Governors of the Federal Reserve System (Board)
Regarding
Docket No. OP-1836

and the
Federal Deposit Insurance Corporation (FDIC)
Regarding
RIN 3064-ZA43

89 FR 61577 (July 31, 2024)

by the

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

Filed on October 30, 2024

Table of Contents

I. Executive Summary

The National Consumer Law Center ("NCLC"),[1] on behalf of its low-income clients, is pleased to respond to the Office of the Comptroller of the Currency's (OCC), the Board of Governors of the Federal Reserve System's (Board), and the Federal Deposit Insurance Corporation's (FDIC), (collectively "the Agencies") Request for Information on Bank-Fintech Arrangements Involving Banking Products and Services Distributed to Consumers and Businesses.[2]

These comments focus on the risk of bank-fintech arrangements that involve payments, deposits, and other types of accounts that hold funds. Separate comments address the risks of credit products.

Many risks posed by bank-fintech arrangements as outlined in the background information to the request for information are cause for concern. Many of these risks negatively impact consumers, especially the most vulnerable.

Bank-fintech arrangements pose an increased risk to a bank's ability to comply with consumer protection laws. Fintech companies lack adequate supervision, increasing the risk of consumer harm. And nonbank entities and crypto firms that partner with banks to engage in banking activities create consumer confusion, especially regarding FDIC insurance.

Questions surrounding a fintech's use and ownership of consumer data and information also increase the risk of harm to consumers. Although many argue that the use of transactional data will lead to the expansion of access to financial services by underserved consumers, this outcome is not guaranteed. Guard rails are still needed around the use of transactional data, which has its limits in promoting financial inclusion and reducing racial disparities. Furthermore, the use and ownership of consumer data by fintech companies can create legal risks for partner banks and privacy risks to consumers.

Additionally, the rapid growth of a bank due to a bank-fintech arrangement can impede a bank's ability to adequately scale compliance and risk management resources, potentially resulting in a failure to comply with applicable laws and regulations and harming consumers and threatening the safety and soundness of the U.S. financial marketplace. This is especially true when bank-

---

[1] Since 1969, the nonprofit National Consumer Law Center® (NCLC®) has used its expertise in consumer law and energy policy to work for consumer justice and economic security for low-income and other disadvantaged people in the United States. NCLC's expertise includes policy analysis and advocacy; consumer law and energy publications; litigation; expert witness services, and training and advice for advocates. NCLC works with nonprofit and legal services organizations, private attorneys, policymakers, and federal and state government and courts across the nation to stop exploitative practices, help financially stressed families build and retain wealth, and advance economic fairness. NCLC publishes a series of consumer law treatises, including *Consumer Banking and Payments Law* (7th ed. 2024), updated at library.nclc.org. These comments were written by Carla Sanchez-Adams.

[2] The Notice of Proposed Rulemaking is available at https://www.federalregister.gov/documents/2024/07/31/2024-16838/request-for-information-on-bank-fintech-arrangements-involving-banking-products-and-services#footnote-14-p61582 and published at 89 FR 61577 (Jul. 31, 2024).

fintech arrangements increase the risk of Bank Secrecy Act (BSA) non-compliance, including where bank-fintech arrangements make it difficult to protect consumers from payment fraud.

II. Bank-fintech arrangements pose a risk to banks' ability to comply with consumer protection laws because fintech companies lack adequate supervision, increasing the risk of consumer harm.

Emerging payment systems fulfill the same purpose as their predecessors, and nonbank entities offer many of the same consumer payment services that banks do. They should not receive different treatment from regulators, and they need the same oversight.[3] Payment apps and digital wallets are used for personal, family, and household purposes to exchange value linked to a deposit, stored value account, credit account, or other form of an account used by consumers to conduct transactions. Oversight is needed to ensure payment apps and digital wallet providers comply with the EFTA, laws against unfair, deceptive, and abusive practices, and other laws.

Consumers are exposed to unfair, deceptive, and abusive practices in the payments area, for example, when consumers are misled to believe money stored in a payment app or wallet has the same level of protection as a FDIC-insured bank account, discussed in more detail in Section II. Nonbank payment apps also pose consumer risks with respect to their use of data, as described in Section III below. Additionally, and as discussed in Section VI, supervision is greatly needed to protect consumers from payment fraud and ensure compliance with the BSA. Payment fraud is an ever-present and increasing risk to consumers,[4] and the response to payment fraud by some of the largest players in the digital payments market is inconsistent at best and possibly non-compliant.[5] EFTA violations are extremely common, even among banks that are closely supervised by regulators.[6]

---

[3] The Consumer Financial Protection Bureau (CFPB) issued a proposed rule to define larger participants of a market for general-use digital consumer payment applications which closed on January 8, 2024. The proposed rule may lead to greater supervision of some nonbank payment services, though not all. *See* NCLC *et al*., Comments to the CFPB's Proposed Rule Defining Larger Participants of a Market for General-Use Digital Consumer Payment Applications, Docket No. CFPB-2023-0053 (Jan. 8, 2024) available at https://www.nclc.org/wp-content/uploads/2024/01/240108-CFPB-Payments-App-Comment-Final.pdf.

[4] TransUnion. "TransUnion Report Finds Digital Fraud Attempts Spike 80% Globally From Pre-Pandemic Levels," March 15, 2023. https://newsroom.transunion.com/transunion-report-finds-digital-fraud-attempts-spike-80-globally-from-pre-pandemic/.

[5] Brown, Sherrod, Elizabeth Warren, and Jake Reed. "Brown, Reed, Warren Urge Venmo, Cash App to Reimburse Victims of Fraud and Scams | United States Committee on Banking, Housing, and Urban Affairs," December 14, 2023. https://www.banking.senate.gov/newsroom/majority/brown-reed-warren-urge-venmo-cash-app-to-reimburse-victims-of-fraud-and-scams.

[6] *See*, e.g., Consumer Fin. Prot. Bureau, Supervisory Highlights at 15 (Summer 2021), *available at* www.consumerfinance.gov (stating that "Supervision continues to find violations of EFTA and Regulation E that it previously discussed in the Fall 2014, Summer 2017, and Summer 2020 editions of Supervisory Highlights, respectively," (Listing several violations)); Scott Sonbuchner, Examiner, Fed. Reserve Bank of Minneapolis, Consumer Compliance Outlook, Error Resolution and Liability Limitations Under Regulations E and Z; Regulatory

Yet newer fintech companies, including technology providers and payment apps, do not receive the same type of supervision as other financial institutions in the United States. The Consumer Financial Protection Bureau (CFPB) has proposed to commence consumer protection supervision of the larger participants in the market for general-use digital consumer payment applications.[7] However, that proposed rule has not been finalized; has gaps[8]; only addresses the larger participants; and will only address supervision of consumer protection laws within the CFPB's jurisdiction, not the BSA or other laws overseen by the bank regulators.

Crypto firms also lack sufficient supervision to protect consumers and prevent risks to their bank partners. Several large, well-capitalized crypto firms have claimed that their business model is focused on making crypto and blockchain-based ledgers a mainstream payment method for American consumers.

For example, PayPal has created a stablecoin expressly intended to facilitate consumers' purchase of household goods and services,[9] while another crypto "native" firm, Coinbase, has created a platform where retail merchants are provided crypto wallets that can receive direct crypto payments from customers, without the need to convert crypto assets into fiat currency to settle the transaction.[10] Reports claim that the platform processes payments for thousands of merchants, for 'on-chain' payments worth billions of dollars.[11]

Payments to or from consumers involving crypto should be subject to the EFTA. Various intermediaries active in the crypto space, including crypto wallet providers, exchanges, and others, provide services – including fund transfers – for personal, family or household use, which are the same as or equivalent to those provided by non-crypto digital wallet providers and payment apps. While the EFTA coverage of crypto-assets is currently unsettled and fairly

---

Requirements, Common Violations, and Sound Practices (2d issue 2021), *available at* www.consumercomplianceoutlook.org.

[7] *See* CFPB, Defining Larger Participants of a Market for General-Use Digital Consumer Payment Applications, Proposed Rule, 88 Fed. Reg. 80197 (Nov. 17, 2023).

[8] *See* Comments of NCLC et al on the CFPB's Proposed Rule to Define a Market for General-Use Digital Consumer Payment Applications (Jan. 8, 2024), https://www.nclc.org/resources/comments-on-the-cfpbs-proposed-rule-to-define-a-market-for-general-use-digital-consumer-payment-applications/.

[9] PayPal. "Designed for Payments. 1 USD: 1 PYUSD on PayPal." PayPal Stablecoin | US Dollar Cryptocurrency. Accessed January 5, 2024. https://www.paypal.com/us/webapps/mpp/digital-wallet/manage-money/crypto/pyusd.

[10] Coinbase. "A New Standard in Global Crypto Payments: Coinbase Commerce." Accessed January 5, 2024. https://www.coinbase.com/commerce.

[11] Akolkar, Bhushan. "New Payments Protocol for Coinbase Commerce to Facilitate Instant Crypto Settlements." *CoinGape* (blog), November 17, 2023. https://coingape.com/new-payments-protocol-for-coinbase-commerce-to-facilitate-instant-crypto-settlements/.

complex,[12] banks that engage with fintechs in the crypto area involving payments bear the risk that they could be found in violation of the EFTA.[13]

Even aside from potential EFTA compliance, there is ample evidence to suggest that consumers would benefit from more supervision of crypto actors involved in payments and funds transfers. For example, several crypto firms that suffered losses or became insolvent during the 2022 crash in the crypto markets engaged in practices many believe were unfair, abusive, or deceptive.[14] Additionally, as the crash ensued, there were many reports of customers of these platforms facing challenges accessing or using the digital assets these platforms had retained custody of via their hosted wallets.

The same vulnerability applies to consumers who hold "bank accounts" through nonbank banking apps managed by companies like Chime, Current, Aspiration, Dave, and Money Lion. These tend to be low-income consumers targeted for being unbanked, often receiving sign-up pitches focused on "fee-free" or "interest-free" overdrafts or cash advances that turn out not to be free for most.[15] The banks that issue these accounts are typically small banks, and the nonbank program managers and servicers currently have no federal supervision. These companies, too, have faced problems[16] and enforcement action.[17]

It is also important that bank-fintech partnerships do not exploit the lack of supervision of fintech companies to harm consumers or allow fintech companies to conduct business in such a way as to find loopholes or exclusions from being covered entities under certain regulations that protect consumers. For example, the CFPB stepped up its enforcement of unfair, deceptive, or abusive practices involving overdraft fees and non-sufficient funds fees[18] and proposed new rules on

---

[12] *See* National Consumer Law Center, Consumer Banking & Payments Law § 7.3.2.10 (7th ed. 2024), updated at library.nclc.org.

[13] *See* Nero v. Uphold, 688 F. Supp. 3d 134 (S.D.N.Y. 2023). *See also* Rider v. Uphold HQ, Inc., 657 F. Supp. 3d 491 (S.D.N.Y. 2023) (earlier decision in same case).

[14] Federal Trade Commission. "FTC Reaches Settlement with Crypto Company Voyager Digital; Charges Former Executive with Falsely Claiming Consumers' Deposits Were Insured by FDIC." Federal Trade Commission, October 12, 2023. https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-reaches-settlement-crypto-company-voyager-digital-charges-former-executive-falsely-claiming.

[15] *See* Comments of National Consumer Law Center on Overdraft Lending at Very Large Financial Institutions Comments to the Consumer Financial Protection Bureau, Docket No. CFPB-2024-0002 at 58-61 (Apr. 1, 2024), https://www.nclc.org/wp-content/uploads/2024/04/20240401_Comments_Overdraft-Lending-at-Very-Large-Financial-Institutions-1.pdf.

[16] Kessler, Carson. "A Banking App Has Been Suddenly Closing Accounts, Sometimes Not Returning Customers' Money." ProPublica, July 6, 2021. https://www.propublica.org/article/chime.

[17] Smith, Mary Ann, Daniel P. O'Donnell, and Paul Yee. "Settlement Agreement with Chime Financial." Settlement Agreement. State of California Department of Financial Protection and Innovation, April 4, 2021. https://dfpi.ca.gov/wp-content/uploads/sites/337/2021/04/Admin.-Action-Chime-Financial-Inc.-Settlement-Agreement.pdf.

[18] CFPB, Supervisory Highlights: Junk Fees Update Special Edition, Issue 31 (Fall 2023).

these topics.[19] However, the overdraft rule would only apply to very large financial institutions, and nonbank companies that increasingly offer "bank accounts" to vulnerable consumers would not be subject to the overdraft rule. As such, nonbank companies pose a greater risk of harming consumers by charging overdraft fees that are above the amount a large bank may charge.

Because all these fintech companies lack adequate supervision and increase the risk of consumer harm, bank-fintech arrangements increase the risk that banks may fail to adequately comply with consumer protection laws.

III. Nonbank entities engaging in banking activities and crypto firms increase the risk of end-user confusion, especially regarding FDIC insurance.

NCLC provided comments in support of the FDIC's proposed rule which would amend subpart B of the Federal Deposit Insurance Act to expressly address which statements or omissions constitute a misrepresentation.[20] As the FDIC noted in its proposed rule, nonbanks have increasingly misused the official FDIC advertising statement, FDIC-associated terms, and FDIC-associated images to the detriment of consumers.[21] For example, Cash App previously advertised on its website that "with a Cash Card, your Cash balance is FDIC-insured through our partner banks, which means the federal government promises to protect it."[22] This is misleading insofar as Cash App failed to explain that many funds held through the Cash App are not insured. It is also possible that funds accessed through the Cash Card are not continuously held in insured accounts with pass-through insurance and may be transferred from Cash App's non-FDIC insured accounts to insured accounts when purchases are made. Such representations by nonbanks can be false and misleading and present a high risk of confusing consumers as to whether they are dealing with an insured depository institution and whether deposit insurance applies to their funds.[23]

Some crypto firms have also actively engaged in misleading communications to their customers and clients regarding whether their products received deposit insurance coverage. The FDIC sent cease and desist letters to several firms, including FTX.US, claiming the firms falsely suggested

---

[19] Consumer Financial Protection Bureau's Proposed Rules on Overdraft Lending: Very Large Financial Institutions, 89 FR 13852 (Feb. 23, 2024), and Proposed Rule on Fees for Instantaneously Declined Transactions, 89 FR 6031 (Jan. 21, 2024).

[20] *See* NCLC *et al.*, Comments to the FDIC's Request for Information Regarding the FDIC Official Sign and Advertising Requirements, False Advertising, Misrepresentation of Insured Status, and Misuse of the FDIC's Name or Logo, Document No. 2022-27349 RIN 3064-AF26 available at https://www.nclc.org/wp-content/uploads/2023/04/2023.04.6-FDIC-Comment.pdf.

[21] *See, e.g.*, FDIC, "FDIC Issues Cease and Desist Letters to Five Companies For Making Crypto-Related False or Misleading Representations about Deposit Insurance" (Aug. 19, 2022), https://www.fdic.gov/news/press-releases/2022/pr22060.html.

[22] Cash App, https://cash.app/bank (last accessed March 21, 2023).

[23] *See* Federal Deposit Ins. Corp., Banking with Third-Party Apps (June 2024), https://www.fdic.gov/resources/consumers/consumer-news/2024-06.html.

on their websites and social media accounts that certain crypto-related products were FDIC-insured, or that stocks held in brokerage accounts were FDIC-insured.[24] The FDIC sent a similar note earlier in 2022 to the once large and now bankrupt crypto lending platform Voyager Digital, demanding that the firm stop making inaccurate claims that customer-held crypto-assets were protected by the government.[25] We believe the agency took appropriate action here, but this pattern of activity underscores the need to make it clear that bank-fintech arrangements do increase the risk of end-user confusion, especially with regard to FDIC insurance.

We strongly encourage the Agencies to (1) require nonbanks to clearly, conspicuously, and continuously disclose that they are not a bank and that their non-deposit products are not insured by the FDIC,[26] (2) prohibit nonbanks from using the words "banking" and "bank account" to describe their products or services offered,[27] and (3) require nonbanks to disclose that even if they partner with an FDIC-insured bank, customer funds sent to the nonbank are not FDIC-insured unless and until the nonbank deposits them in an FDIC-insured bank and holds them in a manner in which they are eligible for pass-through insurance.[28] Failure by a nonbank to comply with any of the above should constitute a material omission and be considered a deceptive practice.

IV. The use and ownership of consumer data and information by fintechs create an increased risk to consumers and partner banks.

A. Fintechs collect extensive consumer data with little oversight, creating legal risk for partner banks and privacy risks to consumers.

As mentioned in the request for information, "Bank-fintech arrangements often rely on new, innovative, and potentially untested uses of data to expand or enhance access to financial

---

[24] *See* FDIC, "FDIC Issues Cease and Desist Letters to Five Companies For Making Crypto-Related False or Misleading Representations about Deposit Insurance" (Aug. 19, 2022), https://www.fdic.gov/news/press-releases/2022/pr22060.html.

[25] *See* Banking Dive, "FDIC probes Voyager's language surrounding deposit insurance." July 8, 2022, available at https://www.bankingdive.com/news/fdic-probes-voyagers-language-surrounding-deposit-insurance/626865/.

[26] Although many nonbanks already disclose that they are not a bank, they do so in fine print footnotes unlikely to be read by consumers. *See, e.g.*, Chime, https://www.chime.com/about-us/ (last accessed March 21, 2023) (Chime discloses in fine print on its sub-page, "About Us," that it "is a financial technology company, not a bank. Banking services and debit card provided by The Bankcorp Bank, N.A. or Stride Bank, N.A."); Money Lion, https://www.moneylion.com/ (last accessed March 21, 2023) (MoneyLion discloses in fine print that although it "is a financial technology company, not a bank, RoarMoney is powered by Pathward, N.A., Member FDIC.").

[27] *See, e.g.*, mobile finance apps, Porte, https://www.joinporte.com/ (last accessed March 21, 2023) ("Banking built for you. Porte believes your banking experience is about more than money. With account alerts, charitable giving, and mobile capture, we've built a mobile banking experience around you. Download the app today to open an account.").

[28] *See, e.g.*, Chime, https://www.chime.com/checking-account/ (last accessed March 21, 2023) ("Chime accounts are insured up to the standard maximum deposit insurance amount of $250,000 through our partner banks, Strike Bank, N.A. or the Bancorp Bank, N.A., Members FDIC.").

services, which may in turn lead to risks related to compliance with laws and regulations, operational challenges, and the ownership, use, and nature of that data. Introducing alternative data into a bank's existing systems may pose risks," for example, a "bank's ability to address concerns associated with alternative data and its use (including as to accuracy and biases)."[29]

Many fintech companies rely on data collection for their sustainability. They collect personal information because their platforms permit it and can also seek other forms of data (*e.g.*, web browsing, social media, educational background). Banks do not have the broad-reaching platforms or aggressive data collection compared to fintechs that can gather and analyze a consumer's activities in multiple forums, including at different depository institutions. To compete against their peers, fintech companies race to mine the data and exploit its contents in ways consumers would not expect or authorize for maximum profit. For example, payment apps and digital wallet providers can use consumer information to create new financial products.[30]

Additionally, a fintech can monetize payment data when adding it to other information already in a consumer's profile. With payment data, fintech companies can expand the totality of their knowledge about a consumer; the addition of payment data adds value to pre-existing non-payment data. Payment data includes (but is not limited to) transaction amounts, timing, vendor, location, and type of account.

There are valuable pro-consumer uses for payment data, such as informing fraud analytics.[31] But without clear guidance about the use of consumer payment data for fraud analytics, innocent consumers may be harmed.[32] Furthermore, fintech companies stand to use this information in ways that pit their interests against those of consumers and other end users.[33]

Financial institutions that are subject to supervision have oversight to ensure that they comply with data privacy laws and are not engaging in unfair, deceptive or abusive practices. Banks are supervised for compliance with the Fair Credit Reporting Act, Gramm-Leach-Bliley Act, UDAAP laws, and other laws dealing with data privacy. The CFPB, the Federal Reserve, and

---

[29] 89 FR 61577 (Jul. 31, 2024) at 61583.

[30] By way of illustration, Apple analyzed payment activity in Apple Pay to help it build a new buy now pay later service. It launched the service in 2023, incorporating it inside its digital wallet platform. Apple Newsroom. "Apple Introduces Apple Pay Later," March 28, 2023. https://www.apple.com/newsroom/2023/03/apple-introduces-apple-pay-later/.

[31] JPMorgan Chase. "Payments Data for Fraud Detection." Artificial Intelligence Initiatives. Accessed December 19, 2023. https://www.jpmorgan.com/technology/artificial-intelligence/initiatives/synthetic-data/payments-data-for-fraud-detection.

[32] For a more in-depth discussion about the impact of fraud screening on consumers, *see* written testimony of Carla Sanchez-Adams before the U.S. Senate Committee on Banking, Housing and Urban Affairs, "Examining Scams and Fraud in the Banking System and Their Impact on Consumers," p. 30-33, available at https://www.nclc.org/wp-content/uploads/2024/02/Written-testimony-The-Problem-of-Payment-Fraud.pdf.

[33] Gam, Boaz. "The Importance of Payments Data for Businesses." Payneteasy, April 19, 2023. https://payneteasy.com/blog/why-is-payments-data-the-key-to-understanding-your-customers.

other federal regulators have held banks accountable for not protecting data. As a result, traditional financial institutions approach data with caution.

While fintech companies may be covered by the same laws, they do not have the same oversight to ensure compliance. That lack of oversight and the potential for legal violations and unfair, deceptive or abusive practices creates risks for banks.

The CFPB just finalized strong protections pursuant to Section 1033 of the Dodd-Frank Act governing when bank account data and data from other financial accounts is shared with a consumer's permission.[34] These protections include:

- bank account data can only be used for the purpose for which the consumer granted permission;
- the user of the data can only obtain as much data as necessary for the permissioned use, i.e., a data minimization standard; and
- the user is prohibited from engaging in secondary use of the data, *i.e.* the data can only be used for the reason that the consumer gave permission. The latter prohibition prevents the sale of the data or its use for cross-marketing.

Yet these Section 1033 protections will only apply when financial account data is shared pursuant to the consumer's permission. There is still a risk that data will be shared without the consumer's permission. Moreover, Section 1033 only applies to financial account data, and fintechs collect other types of data that will not be subject to the 1033 protections.

Outside of Section 1033, the primary statutory protection that prevents financial institutions from selling data without a consumer's permission is the Gramm Leach Bliley Act (GLBA). GLBA is a much less protective statute because it only allows the consumer to opt out of some, but not all, secondary uses.[35]

---

[34] CFPB, Press Release, CFPB Finalizes Personal Financial Data Rights Rule to Boost Competition, Protect Privacy, and Give Families More Choice in Financial Services (Oct. 22, 2024), https://www.consumerfinance.gov/about-us/newsroom/cfpb-finalizes-personal-financial-data-rights-rule-to-boost-competition-protect-privacy-and-give-families-more-choice-in-financial-services/.

[35] 15 U.S.C. § 6802(b). *See generally*, National Consumer Law Center, Fair Credit Reporting § 18.4.1.14 (10th ed. 2022), updated at www.nclc.org/library.

B. Transactional data has promising uses but the data is sensitive, needs protection, and will reveal racial disparities.

Deposit accounts are one source of alternative data not found in the traditional credit reports provided by the Big Three credit bureaus.[36] This data can include rent and utility payments and bank account transactions.

Bank account transaction and cashflow information holds promise as a form of alternative data. Research has shown that this data has the potential to help identify consumers, including borrowers of color, who have the ability to repay credit but might otherwise face constraints on their ability to access credit.[37] In particular, cashflow data may help the tens of millions of consumers who do not have a credit history with the "Big Three" credit bureaus, *i.e.*, Equifax, Experian, and TransUnion, or have histories are too scant or old ("thin") to generate a credit score.[38] In terms of racial disparities, about 15 percent of Black and Latino consumers have no credit history compared to 9 percent of white consumers; another 13 percent of Blacks and 12 percent of Latinos consumers are unscorable compared to 7 percent of white consumers.[39]

However, bank account transaction data can also be very sensitive and revealing and thus needs strong consumer protections. The data might show when the consumer gets paid, where they shop, what advocacy organizations they support, or which healthcare providers they use. The new Section 1033 rules should help, but vigilance is still needed to protect against inappropriate collection and uses of data that infringe on consumers' privacy, potentially have disparate impacts, or result in unfair, deceptive or abusive practices.

Moreover, we must be careful with the use of bank account data because it will almost certainly exhibit disparities by race. A key factor likely to be used by cashflow scoring models is overdrafts, and consumers of color are disproportionately affected by bank overdraft practices. As compared with white consumers, Black consumers are 69 percent more likely and Latino consumers are 60 percent more likely to reside in a household charged at least one overdraft or NSF fee in the past year.[40]

---

[36] Consumer Fin. Prot. Bureau, Request for Information Regarding Use of Alternative Data and Modeling Techniques in the Credit Process, 82 Fed. Reg. 11,184 (Feb. 21, 2017) (defining alternative data as information not typically found in consumer's credit files at nationwide CRAs).

[37] FinRegLab, The Use of Cash-Flow Data in Underwriting Credit (July 2019) https://finreglab.org/wp-content/uploads/2019/07/FRL_Research-Report_Final.pdf.

[38] Consumer Fin. Prot. Bureau, Data Points: Credit Invisibles, 6 (May 2015), https://files.consumerfinance.gov/f/201505_cfpb_data-point-credit-invisibles.pdf

[39] *Id.*

[40] Consumer Fin. Prot. Bureau, Overdraft and Nonsufficient Fund Fees: Insights from the Making Ends Meet Survey and Consumer Credit Panel, 25 (Dec. 2023) https://files.consumerfinance.gov/f/documents/cfpb_overdraft-nsf-report_2023-12.pdf. The CFPB has proposed reforms to lower the cost of overdraft fees and reduce the incentive to engage in abusive overdraft practices, but the proposed rule would not apply to the smaller financial institutions that

Having a credit score is not an end in itself and can generate its own problems. A low credit score can attract predatory credit offers, which only harm consumers' financial health. Low credit scores can also be problematic due to the myriad ways credit scores are used, such as in employment and insurance.

Cashflow data, for example, may not be equally available to all consumers. Black and Latino consumers are disproportionately unbanked – 11.3 percent of Black households and 9.3 of Latino households were unbanked compared to 2.1 percent of white households.[41] Being unbanked, of course, excludes consumers from the possibility of using cashflow data.

C. Alternative data has its limits in promoting financial inclusion and reducing racial disparities.

"Alternative data" is often promoted as a solution to credit invisibility, racial disparities and financial exclusion. However, while alternative data can sometimes be helpful to some consumers, it can also be extremely harmful to other consumers dealing with the consequences of living in financial precarity. The benefit versus harm depends on the type of data, how it is supplied, and how it is used.

Alternative data will likely only have limited impact on promoting financial inclusion for the most vulnerable consumers. Low- and moderate-income (LMI) consumers deal with a host of financial struggles and challenges that prevent their economic advancement, such as insufficient and unstable incomes; little or no assets; unaffordable and ever-increasing rents; high childcare costs; burdensome medical and prescription costs; and more. These struggles to obtain financial wellbeing must all be addressed before LMI consumers are truly "included."

Another, perhaps more complex, side of this financial inclusion problem is the racial credit score gap. When Black and Latino consumers do have credit scores, the scores reflect dramatic and troubling disparities by race. A 2019 study by the Urban Institute found that over 50 percent of white households have credit scores over 700, but only 20 percent of Black households do.[42] A multitude of older studies show similar results, while the Urban Institute's Debt in America map

---

typically partner with fintech companies. Consumer Fin. Prot. Bureau, Overdraft Lending: Very Large Financial Institutions, (Jan. 17, 2024) https://www.consumerfinance.gov/rules-policy/rules-under-development/overdraft-lending-very-large-financial-institutions-proposed-rule/#:~:text=The%20Consumer%20Financial%20Protection%20Bureau,of%20similarly%20situated%20products%2C%20unless.

[41] Fed. Deposit Ins. Corp., 2021 FDIC National Survey of Unbanked and Underbanked Households, 2 (July 24, 2023), (Table ES.2) https://www.fdic.gov/analysis/household-survey/2021report.pdf.

[42] Choi, Jung Hyun, et. al., "Explaining the Black-White Homeownership Gap: A Closer Look at Disparities across Local Markets," Urban Inst., 8 (Nov. 2019), https://www.urban.org/research/publication/explaining-black-white-homeownership-gap-closer-look-disparities-across-local-markets.

consistently shows racial disparities in debts in collection, which translate into lower scores.[43] The racial disparities in credit scores are due to deep structural factors, including the racial wealth gap,[44] decades of redlining and housing segregation,[45] historical and present-day employment discrimination,[46] and racially biased criminal justice practices.[47] Put simply, the data inputs in our credit scoring system are also stratified by race.

The limits of alternative data are illustrated by a Government Accountability Office (GAO) study examining the impact of alternative data in qualifying more consumers for mortgages. The GAO noted that while alternative data could "improve or generate scores for [credit invisible or low scoring] consumers, it is unclear whether the increases would be sufficient to qualify many additional consumers for lower-cost mortgages."[48] The GAO also noted that nearly half (48 percent) of unscorable consumers were under 24 or over 65 years old, which the GAO characterized as "age groups less likely than most to be seeking mortgage credit."[49]

As for racial disparities in credit scores, alternative data will not eliminate them, and it is not a panacea for credit inequities. Any data that relies on financial information will still reflect racial disparities given the unequal economic positions of households of color and white households.

To combat such disparities, credit scoring models need to be refined and improved with intentionality. Intentionality is key— the income disparities and wealth gaps reflected by credit scores are the product of centuries of intentional discrimination. They cannot and will not be reduced or resolved without the same level of intentionality. Without intentionality, feeding

---

[43] Urban Inst., Debt in America: An Interactive Map, https://apps.urban.org/features/debt-interactive-map/?type=overall&variable=totcoll (last visited Feb. 20, 2024) (22% of white communities have debts in collection versus 35% in communities of color). These racial disparities show up consistently when data is examined from individual states and localities.

[44] Aladangady, Aditya, Chang, Andrew C., and Krimmel, Jacob, "Greater Wealth, Greater Uncertainty: Changes in Racial Inequality in the Survey of Consumer Finances," https://www.federalreserve.gov/econres/notes/feds-notes/greater-wealth-greater-uncertainty-changes-in-racial-inequality-in-the-survey-of-consumer-finances-20231018.html ("The typical White family had about six times as much wealth as the typical Black family, and five times as much as the typical Hispanic family/") (last visited Feb. 20, 2024).

[45] Rothstein, Richard. The Color of Law: A Forgotten History of How Our Government Segregated America. United Kingdom, Liveright, 2017.

[46] Weller, Christian E. "African Americans Face Systematic Obstacles to Getting Good Jobs, Center for American Progress," https://www.americanprogress.org/article/african-americans-face-systematic-obstacles-getting-good-jobs/ (last visited Feb. 20, 2024).

[47] Balko, Radley, "There's overwhelming evidence that the criminal justice system is racist. Here's the proof," Wash. Post (June 10, 2020) https://www.washingtonpost.com/graphics/2020/opinions/systemic-racism-police-evidence-criminal-justice-system/.

[48] Gov't Accountability Off., Mortgage Lending: Use of Alternative Data Is Limited but Has Potential Benefits, 14 (Nov. 2021), https://www.gao.gov/assets/gao-22-104380.pdf.

[49] *Id.*

financially-based data with racial disparities into algorithms or machine learning models will instead replicate or amplify those disparities.

Most critically, there must be efforts to reduce the racial disparities in the underlying factors that create the divide in credit scores and other financial data— i.e., reducing the racial wealth gap, combatting housing segregation, preventing employment discrimination, and implementing criminal legal system reforms. The experience during the COVID-19 pandemic is instructive. With two stimulus payments and expanded federal unemployment benefits, credit scores stayed stable and even went up for some consumers.[50] The lesson is simple: if consumers have more financial resources, they can better pay their bills and their scores go up. Racism and its legacy drain precious resources from communities of color, which is directly reflected in credit scores and other financial data.

V. Bank-fintech arrangements pose a risk to consumers and to the safety and soundness of the U.S. financial marketplace when growth is too rapid.

Banks that partner with fintechs may use their charter to attract revenue and grow quickly but without the cost of serving consumers. However, this approach to attracting deposits creates meaningful risk to a bank's safety and soundness and/or its ability to comply with applicable laws and regulations, including consumer protection laws.

One of the biggest examples of harm to consumers when bank-fintech arrangements go awry is the collapse of Synapse. Synapse partnered with Evolve Bank, which the Federal Reserve supervises. However, even under the Federal Reserve's supervision, Evolve failed to mitigate the risk that Synapse posed to consumers. Even though the Federal Reserve issued an enforcement action against Evolve Bancorp, Inc. and Evolve Bank & Trust for deficiencies in the bank's anti-money laundering, risk management, and consumer compliance programs, consumers impacted by the collapse of Synapse were not made whole after the fact.

VI. Bank-fintech arrangements increased the risk of non-compliance with the Bank Secrecy Act, making it difficult to protect consumers from payment fraud.

Financial institutions have responsibilities to know their customers and monitor transactions to comply with the BSA and implementing Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) regulations, as briefly mentioned in the request for information.[51] However, the BSA program requirements are much more stringent for banks than for the other types of entities that engage in bank-fintech arrangements.[52] In comments filed with FinCEN,[53]

---

[50] NCLC, The Credit Score Pandemic Paradox and Credit Invisibility, (Feb. 2021), https://www.nclc.org/wp-content/uploads/2022/10/IB_Pandemic_Paradox_Credit_Invisibility.pdf

[51] *See* 89 FR 61577 (Jul. 31, 2024) at 61581.

[52] *Id.* at 61579 to 61581.

[53] NCLC Comments on FinCEN's Rulemaking on Anti-Money Laundering and Countering the Financing of Terrorism, Docket Number FINCEN–2024–0013 (Jul. 3, 2024), available at

NCLC urged FinCEN to expand the Customer Identification Program (CIP) and customer due diligence (CDD) requirements for entities other than banks that engage in payment and banking services, such as person-to-person (P2P) payment apps, payment processors, fintech companies offering banking as a service or offering bank-like services, and crypto-related entities including crypto exchange platforms.

Banks may partner with nonbanks involved in P2P payments in various ways. They may hold funds in accounts with or without FDIC pass-through insurance payable to the consumer; issue debit cards and connected bank accounts; or process payments in other ways. But the fraud prevalent in P2P services poses risks to consumers.

P2P payment apps have become increasingly popular among consumers. Seventy-six percent of households use Venmo or Cash App.[54] In addition to P2P payment services, consumers are also increasingly adopting other forms of technology to make payments.[55] These newer payment apps and technologies are accepted by more retailers, demonstrate a rapid growth trajectory, are situated within platforms with other financial services, and are being structured to work with crypto.

These platforms have become fertile ground for fraudsters and organized crime, posing risks to consumers and law enforcement. According to the Federal Trade Commission (FTC),[56] "payment app or service" is the third largest category of payment method specified by fraud victims in terms of number of reports (after credit cards and debit cards) for all of 2023, and the second largest category of payment method specified by fraud victims in terms of number of reports (after credit cards) for the first two quarters of 2024. [57] The CFPB has also seen high growth in complaints about fraud in P2P apps and digital wallets.[58] As consumer, small business,

---

https://www.nclc.org/resources/comments-on-fincens-proposed-rule-on-anti-money-laundering-and-countering-the-financing-of-terrorism-programs/.

[54] Anderson, Monica, "Payment Apps like Venmo and Cash App Bring Convenience – and Security Concerns – to Some Users," Pew Research Center (blog), (Sept. 8, 2022), available at https://www.pewresearch.org/short-reads/2022/09/08/payment-apps-like-venmo-and-cash-app-bring-convenience-and-security-concerns-to-some-users/.

[55] Chen, Jane, Mahajan, Deepa, Nadeau, Marie-Claude and Varadarajan, Roshan, "Consumer Digital Payments: Already Mainstream, Increasingly Embedded, Still Evolving," Digital Payments Consumer Survey, (Oct. 20, 2023), available at https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/consumer-digital-payments-already-mainstream-increasingly-embedded-still-evolving.

[56] Reports of fraud to the FTC do not always specify the payment method utilized to perpetuate the fraud; however, the FTC does collect and report data on payment method when available.

[57] FTC fraud reports by payment method, available at https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods. For 2023, only 474,328 (18%) of 2,606,042 fraud reports received by the FTC specified the payment method. For the first two quarters of 2024, only 222,540 (21%) of 1,085,474 fraud reports received by the FTC specified the payment method.

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

civil rights, community, and legal service groups described at greater length in comments submitted to the Federal Reserve Board and the CFPB, the existing P2P payment systems of large technology companies and financial institutions simply are not safe for consumers to use.[59]

P2P fraud has a particularly harsh impact on low-income families and communities of color. These communities, already struggling and often pushed out of the traditional banking system, can least afford to lose money to scams and errors. Because many people of color are also unbanked or underbanked,[60] they are the target audience for use of many of the P2P apps. For example, a September 2022 Pew Research Center survey shows that 59% of Cash App users are Black and 37% are Hispanic.[61] Cash App has been subject to reports of widespread fraud,[62] failing to protect the very vulnerable populations it targets.

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

- Manhattan District Attorney Alvin Bragg explains how criminals have utilized deception, violence, or threat of violence to steal funds from consumers through payment apps like Cash App.[63]

- 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

---

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

[60] 11.3 percent of Black and 9.3 percent of Latino households are unbanked compared to only 2.1% of white households. *See* FDIC, 2021 FDIC National Survey of Unbanked and Underbanked Households, at 2, available at https://www.fdic.gov/analysis/household-survey/2021report.pdf (last updated Jul. 24, 2023).

[61] Anderson, Monica, “Payment apps like Venmo and Cash App bring convenience – and security concerns – to some users,” Pew Research Center (Sept. 8, 2022), available at https://www.pewresearch.org/short-reads/2022/09/08/payment-apps-like-venmo-and-cash-app-bring-convenience-and-security-concerns-to-some-users/.

[62] Hindenburg Research, “Block: How Inflated User Metrics and ‘Frictionless’ Fraud Facilitation Enabled Insiders To Cash Out Over $1 Billion,” (Mar. 23, 2023), available at https://hindenburgresearch.com/block/. (“Former employees estimated that 40%-75% of accounts they reviewed were fake, involved in fraud, or were additional accounts tied to a single individual”).

[63] Morales, Mark, “Venmo and other payment app theft is ‘skyrocketing,’ *Manhattan DA warns*,” CNN (Jan. 23, 2024), available at https://www.cnn.com/2024/01/23/business/venmo-payment-app-theft?cid=ios_app.

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.[64]

- In a similar fraud scheme, a single mom in South Carolina looking for housing paid a deposit, cleaning fee, and first month's rent on a condo listed on Redfin.com through a payment app and lost $2,600.[65]

Crypto-assets are another large category where reports of fraud are rife. "Cryptocurrency" "is the second largest category of payment method reported by fraud victims to the FTC in terms of number of dollars lost (after bank transfer or payment) for all of 2023 and the first two quarters of 2024.[66]

If CIP and CDD requirements are not enhanced for nonbank entities that engage in payment and banking services, then these entities will continue to pose a risk to any financial institution that partners with them. As such, the Agencies should clarify that bank-fintech arrangements do increase the risk of BSA compliance.

VII. Conclusion

For all the reasons described above, bank-fintech arrangements pose a risk to consumers and, by extension, to the banks engaged in these partnerships. Regulators should continue to take measures to protect consumers from the risks of bank-fintech arrangements and to ensure the safety and soundness of the U.S. financial system.

We appreciate the Agencies' willingness to undertake this effort and are happy to answer questions. If you have any questions, please contact Carla Sanchez-Adams at csanchezadams@nclc.org.

Respectfully submitted,

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

---

[64] Johnson, Tia, "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/.

[65] Cioppa, Jordan, "James Island woman says rental scam cost her $2,600," WCBD News2 (Jan. 10, 2023), available at https://www.counton2.com/news/james-island-woman-says-rental-scam-cost-her-2600/.

[66] FTC fraud reports by payment method, available at https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods. For 2023, roughly $ 1.4 billion was reported as lost due to fraud by cryptocurrency and $678.8 million in the first two quarters of 2024.