Mr. Rohit Chopra  
Director  
Bureau of Consumer Financial Protection  
1700 G Street NW  
Washington, DC 20552  
Via email to BigTechPaymentsInquiry@cfpb.gov

Re: Docket No. CFPB-2021-0017  
Request for Comment Regarding the CFPB’s Inquiry Into Big Tech Payment Platforms

Dear Director Chopra:

Demand Progress Education Fund applauds the Consumer Financial Protection Bureau’s commitment to a thorough investigation of the impact of large technology firms as they develop and use payment systems. Because of the effects that this expansion will have - and in some cases, are already having - on competition, privacy, and small businesses, we urge the Bureau to act to block Big Tech’s ongoing expansion into payment systems. As detailed in these comments, Big Tech companies, particularly Amazon, Apple, Facebook, and Google, have a history of anticompetitive behavior, unfair surveillance, poor data management practices, and invasions of privacy.

Moderate regulation will not prevent Big Tech companies from abusing the power and profit that payment systems grant them. Regulators have too long relied upon behavioral constraints in hopes of allowing companies with monopoly market power to operate multiple lines of businesses while ostensibly guarding against anti-competitive or other abusive business practices. Such efforts have often proved unmanageable,¹ and in some cases constraints imposed by a given administration have been swept aside by subsequent one.² Moreover, a history of recidivism by the largest tech companies are cause for concern that behavioral constraints and subsequent enforcement will not be adequate. The Bureau should therefore, to the extent

allowable, ban ownership of payments systems by the dominant platforms, rather than allow Big Tech companies to operate payment systems with behavioral constraints.

1. Big Tech Payment Systems Further Contribute to Abuses of Dominance and Monopolistic Practices

Consumer financial data is a highly valuable dataset, useful for targeted advertising, credit-risk assessment, and a variety of other purposes.\(^3\) This data contains granular information about spending habits - what consumers buy, when, from whom, and where. This treasure trove of valuable consumer financial data, especially when combined with other datasets, allows Big Tech companies to further expand their market dominance.

Big Tech’s business model relies heavily on monetizing data. Few other businesses, outside of direct banking systems, have access to such comprehensive and commercially valuable payment data as Big Tech companies have while operating payment systems. Even before expanding into payment systems, Big Tech companies already had vast data troves - including locational data, browsing data, social network data, search data, biometric data, and communications data - which gave them significant advantages in the competitive arena. Financial data generated by payment systems can now be aggregated with those other datasets to give Big Tech companies even greater advantages against any potential competitors.

Financial data is particularly valuable in targeted advertising, an area where Big Tech companies have already cemented their monopolistic advantage.\(^4\) This advertising revenue can then be used to offset/subsidize losses in other areas of business, which allows Big Tech companies to further undercut competitors in other spheres of operation. Already, many Big Tech companies are offering free products (for example, Google Maps and Facebook’s social network) in exchange for data collection and related digital advertising. Additionally, ad revenue generated by financial data can also be used to acquire even more data, or more businesses that possess or create data, which can then be used for more acquisitions - a vicious anti-competitive cycle. Even now, the decade-plus of data troves and user adoption advantages make it nearly impossible for other companies to compete with Big Tech.\(^5\) Allowing for the collection of financial data from payment systems exacerbates that problem.

Big Tech companies already have a proven track record of aggressively anti-competitive actions. In fact four of the companies mentioned in the CFPB’s announcement have already been

---


\(^5\) Id. at 40-46
the subject of an intensive investigation by the House Committee on the Judiciary’s Subcommittee on Antitrust, Commercial and Administrative Law. This investigation found that Amazon, Apple, Facebook, and Google routinely engaged in anticompetitive business practices. The Subcommittee’s investigation also revealed that Amazon had acquired competitors, preferred its own products on its platform, and utilized seller data to secure its dominance. The Subcommittee found that Apple used control of its app store to create barriers to competition, had misappropriated competitively sensitive data from app developers, and had used dominance and control of the app store to raise prices. The Subcommittee found that Facebook, for example, had engaged in the acquisition and neutralization of nascent competitive threats and had preferred its own services. Lastly, the Subcommittee investigation revealed that Google was guilty of undermining vertical search providers, using dominance to steadily increase advertising fees, using anti-competitive contracts to block competitors, and utilizing user data in anticompetitive ways to secure its dominance. The Subcommittee concluded that these four companies needed to be broken up and then heavily regulated— including prohibitions on acquisitions of competitors and potential competitors and prohibitions on self-preferencing.

Allowing Big Tech’s continued expansion into payment systems will enable even more market dominance. This would be the opposite of the Subcommittee’s recommendations, which focus on breaking up these companies and heavily regulating any future expansive tendencies.

2. Big Tech payment systems allow companies to expand their pattern of abusive practices toward businesses that use their platforms

Big Tech companies have a long history of engaging in abusive practices toward the businesses that rely on their platforms, and their expansion into payment systems will only create more opportunities for such abusive practices. For example, the expansion into payment systems allows Big Tech companies to use their market dominance to force sellers and consumers to use a given Big Tech company’s payment system, extracting whatever contractual terms are most favorable to the Big Tech company, similar to what Amazon already does with its online marketplace. Payment platforms can permit Big Tech companies to squeeze even more revenue out of businesses and their customers, and accumulate ever more information about business and user behaviors.

Big Tech’s companies’ history of abusive practices toward businesses that use their platforms are well-documented. Amazon, for instance, was recently the subject of a report by the Institute for Local Self Reliance, which showed that “Amazon is exploiting its position as a gatekeeper to impose increasingly steep tolls on these businesses. Using a variety of fees, Amazon now pockets a 34 percent cut of the revenue earned by independent sellers on its

---

6 Id. at 258-259.
site, our analysis found. That’s up from 30 percent in 2018, and 19 percent in 2014.”7 The House Subcommittee on Antitrust, Commercial, and Administrative Law found related abuses, including Amazon’s practice of self-preferencing its own products in Amazon Marketplace search results, its high fees and bullying of sellers,8 its extraction of harmful contract terms from its sellers,9 and its use of third-party seller data to launch competing products10 (including, famously, its copying of Pirate Trading’s tripod, then subsequent banning of Pirate Trading).1112 Amazon’s abusive practices have been the subject of investigations by the Federal Trade Commission and the Attorneys General of California and New York.13

Apple, too, has a rich history of abusive practices toward other companies that use its platform. Apple maintains exclusive control over its app store, an arrangement that has allowed it to raise prices for app developers, bar competitors, and misappropriate competitively sensitive data from those developers.14

Facebook has also behaved in abusive ways toward apps that used its platform. The Antitrust Subcommittee investigation found that when apps that used Facebook’s platform became too popular, the company would often punish them by cutting off the app’s access to the Facebook platform.15

Likewise, Google has taken advantage of its dominance to abuse business users of its platforms, especially in Google Ads and the Google Play Store App market. Google has, for instance, used its dominance to demand exorbitant ad revenues,16 to demand that its own apps be pre-installed on Android devices,17 and to charge very high fees to app developers in its Google Play Store.18

---

The more power these Big Tech companies obtain, the more abuses they engage in. And payment systems - which grant them more data, more of a competitive edge, and more opportunities to demand advantageous and anticompetitive contract terms - only accelerate that dynamic.

3. **Consumer financial data is very sensitive personal information and should not be entrusted to Big Tech companies**

Financial data is among the most sensitive of personal information. Financial data includes purchasing history, which reveals a variety of personal preferences, as well as income and asset information. Purchase and transaction histories can reveal a variety of other sensitive information about individuals, including sexual preferences and identity, religious and political associations, and medical information. And some companies are also already collecting sensitive biometric data as part of their payment systems (for example, Amazon’s One payment system). Entrusting sensitive financial data to Big Tech companies would be unwise because these companies have a history of both purposefully disregarding user privacy (for instance, sharing sensitive information with third parties without user consent) and negligently handling sensitive information in ways which have allowed for data breaches.

Big Tech companies have repeatedly violated user privacy in the pursuit of profit. The FTC has investigated Facebook and Google multiple times for privacy violations and has concluded that Facebook and Google’s repeated privacy violations were unfair and deceptive. Facebook, for instance, repeatedly deceived users about the users’ ability to control their own information. The company actively disregarded user privacy settings, including sharing personal user data with not just users’ friends, but also with third party applications that friends interacted with. Even after coming to a settlement with the FTC in 2012 and pledging to cease its unfair and deceptive privacy practices, Facebook continued to engage in these practices.

---


22 In May 2017, Amazon found that for two years, 24 million customers’ names and American Express numbers were outside a “secure zone” for payment data. And there was no way to know whether the data had been accessed. Aaron Holmes, “533 Million Facebook Users’ Phone Numbers and Personal Data Have Been Leaked Online,” Business Insider, Apr. 3, 2021, https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4

Facebook’s privacy violations and disregard of the 2012 settlement ultimately resulted in the FTC issuing a record-breaking $5 billion fine against the company in 2019.24

Google has been a similarly bad actor on privacy. In 2019, the FTC and the New York Attorney General fined Google and its subsidiary, Youtube, a record-setting $170 million for violations of the Children’s Online Privacy Protection Act.25 This settlement stemmed from Youtube’s collection of personal information from viewers of child-directed channels, without first notifying parents and getting their consent.26 In 2011, the FTC reached another settlement with Google for its unfair and deceptive privacy practices related to its Google Buzz social networking platform, which transformed Gmail users’ private contact lists into publicly viewable contacts without the users’ consent.27

Amazon, Apple, Facebook, and Google have all been the subject of privacy-related lawsuits. Amazon has been sued several times for privacy violations, including violations of children’s privacy related unauthorized listening by the Amazon Alexa Voice Assistant.28 Apple and Google have also been sued for unauthorized listening by their voice assistants, Siri and Google Voice.29 And in 2021, Facebook paid $650 million to settle a class action lawsuit against plaintiffs who claimed it had violated privacy laws by storing biometric data, including facial scans, without getting user approval first.30

Moreover, while the Big Tech companies have demonstrated little respect for the privacy of users, the companies have great respect for their own corporate “privacy” - relying extensively on the secretive transfer of data and the use of hidden (and often discriminatory) algorithms, which determine who is served which information, services, and advertisements.

This raises real questions about the fairness and transparency of the algorithms that govern the payment systems of these Big Tech companies. Big Tech companies already have a

26 Id.
history of discriminatory algorithms (for example, Apple credit card’s line of credit and Google’s discriminatory AI). Secretive data transfer is also a frequent business strategy of these companies - with Facebook’s data transfer (as discussed in its settlement with the FTC) being the most prominent example.

But even when the Big Tech companies are not purposefully disclosing user data, they are often negligently doing so. They have a well-documented history of failing to secure sensitive user data. In Amazon’s case, one Reveal/Wired investigation found “millions of credit card numbers had sat in the wrong place on Amazon’s internal network for years, with the security team unable to establish definitively whether they’d been unduly accessed.” But this story is not an outlier. Facebook recently refused to notify 530 million users whose data was breached by “malicious actors.” And Google agreed to pay a $7.5 million settlement as the result of a class action lawsuit alleging a breach of 500,000 users’ Google+ data. And these are just a few of the cases we know about. As illustrated by Facebook’s refusal to notify its 530 million users, Big Tech companies are not transparent about data breaches and failures to secure data.

Allowing Big Tech companies to expand into payment systems would grant them a trove of highly sensitive data, which they could then exploit at will to generate ever more profit.

4. **Big Tech Companies Should Not be Entrusted with Financial Data Because They Have Often Engaged in Abusive and Dishonest Financial Practices**

Responsibility for payment systems should only be entrusted to companies that have a proven track record of honesty and integrity. Big Tech companies have proven themselves to be decidedly untrustworthy in this area. Amazon, for instance, in the midst of a global pandemic, illegally stole tips from its drivers and was forced by the FTC to send $60 million in payments to

---

35 “Google Agrees to Pay US$ 7.5M Over Google+ Data Breaches,” CISO Mag, Jan. 10, 2020, https://cisomag.eccouncil.org/google-agrees-to-pay-us-7-5m-over-google-data-breaches/
drivers whose tips it had stolen. Both Google and Apple were the subject of substantial FTC “unfair practice” settlements for charging parents for children’s in-app purchases without the parent’s consent. The companies were forced to pay customers back $19 million and $32.5 million, respectively. Amazon was also investigated for similar unfair practices. It seems unwise to entrust payment systems to companies like this who have, in the past, willfully engaged in unfair financial practices and even outright theft.

5. Big Tech Companies Have a History of Developing Poorly Considered Payment Systems and Exploiting Regulatory Ambiguity

Big Tech companies have previously toyed with ideas for poorly-thought-out payment systems, including Facebook’s Diem, earlier called Libra. These systems often amount to shadow banking and attempt to evade the kinds of regulations that typically oversee banks and financial institutions. Diem, in particular, raised questions about regulation and taxation, among them: Would Diem “coins” be securities, overseen by the SEC? Would the stewards of Diem effectively hold themselves out as depository institutions, deserving of FDIC oversight? Would Diem coins be subject to capital gains taxation and thus, difficult to use in most purchasing settings, because purchases would require detailed tracking in order to calculate capital gains taxes?

Other Big Tech payment systems may raise similar concerns. Each payment platform functions differently and requires a tailored complex inquiry into its function - including how purchases should be tracked and taxed, whether the payment currency qualifies as a security or investment, and which agencies should oversee the system. But instead of asking these questions, Big Tech companies have rolled out payment systems in the same thoughtless and haphazard manner that they have rolled out many other products (best summarized by Facebook founder, 

---

41 Id.
42 Id. at 53-56.
43 Id.
Mark Zuckerberg’s “move fast and break things” motto). But financial systems have profound implications not just for users, but for the health of the overall economy, and the gravity of those implications justifies a thoughtful deliberative process before rolling out new payment tools and systems.

6. Big Tech Companies Have Often Broken Commitments to Regulators

Assurances of good faith, consumer protection, and regulatory conformity by Big Tech companies should also be approached with great skepticism. Amazon, Facebook, and Google all have a history of violating their promises to regulators. Google, for example, assured Congress and the FTC that it would not combine Doubleclick data with Google’s other data. That commitment did not last long - in 2016, Google reneged on its promise and combined Doubleclick data with personal information collected by Google’s other services. Facebook has been similarly dishonest with regulators, promising to reform after the FTC’s 2012 order against it, then returning almost immediately to the same unfair and deceptive practices, which ultimately resulted in the FTC’s unprecedented $5 billion fine against the company in 2019. And Amazon has been called out by a bipartisan group of Congressmembers for corporate behavior “that directly contradicts the sworn testimony and representations of Amazon’s top executives—including former CEO Jeffrey Bezos—to the Committee about their company’s business practices during our investigation last Congress.” The Congressmembers condemned the company, stating “[a]t best, this reporting confirms that Amazon’s representatives misled the Committee. At worst, it demonstrates that they may have lied to Congress in possible violation of federal criminal law.”

Big Tech companies cannot be trusted to engage in meaningful self-regulation or even to conform meaningfully to behavioral moderation established by regulations. Any assurances to the contrary ought to be viewed with extreme skepticism.

7. Conclusions

Many past attempts have been made to merely regulate Big Tech companies as they move into ever more business spaces, acquire ever more competitors, gobble up ever more data. These attempts to rein Big Tech in via moderate regulation has proven over and over again to be

45 Id.
48 Id.
ineffective. Big Tech companies consistently violate both norms and the law, they engage in anticompetitive practices and abuse other businesses and consumers, and they make misrepresentations to regulators and Congress - all in the pursuit of profit and dominance. Big Tech companies should not be entrusted with the kinds of sensitive data and choices that are involved in overseeing payment systems. For this reason, CFPB should, to the extent possible under the law, prohibit Big Tech companies from operating payment systems.

Sincerely,
David Segal
Executive Director
Demand Progress Education Fund

Ginger Quintero-McCall
Legal Director
Demand Progress Education Fund
ginger@demandprogress.org