United States Public Interest Research Group (USPIRG) and the Center for Digital Democracy submit these additional comments to further inform the Bureau’s inquiry. They amplify the comments USPIRG and CDD submitted last year.¹

We believe that since we filed our original comment, the transformation of “Big Tech” operated digital payment platforms has significantly evolved, underscoring the need for the Bureau to institute much needed consumer protection safeguards. We had described how online platform based payment services seamlessly incorporate the key elements of “commerce” today—including content, promotion, marketing, sales and payment. We explained how these elements are part of the data-driven “surveillance” and personalized marketing system that operates as the central nervous system for nearly all U.S. online operations. We raised the growing role that “social media commerce” plays in contemporary payment platforms, supporting the Bureau’s examination of Big Tech platforms and consumer financial payment services. For example, U.S. retail social media commerce sales will generate $53 billion in 2022, rising to $107 billion by 2025, according to a recent report by Insider Intelligence/eMarketer. Younger Americans, so-called “Generation Z,” are helping drive this new market—an indicator of how changing consumer financial behaviors are being shaped by the business model and affordances of the Big Tech platforms, including TikTok, Meta and Google.²

In order to meaningfully respond to the additional questions raised by the Bureau in its re-opening of the comment period, in particular regarding how the payment platforms handle “complaints, disputes and errors” and whether they are “sufficiently staffed…to address consumer protection and provide responsible customer service,” USPIRG and CDD offer some further analysis regarding the structural problems of contemporary platform payment systems below.³

**First, payment services such as operated by Google, Meta, TikTok and others have inherent conflicts of interest.** They are, as the Bureau knows, primarily advertising systems, that are designed to capture the “engagement” of individuals and groups using a largely stealth array of online marketing applications (including, for example, extensive testing to identify ways to engage in subconscious “implicit” persuasion).⁴ Our prior comment and those of other consumer groups have already documented the extensive use of data profiling, machine learning, cross-platform predictive analysis and “identity” capture that are just a few of current platform monetization tactics. The continually evolving set of tools available for digital platforms to target consumers has no limits—and raises critical questions when it comes to the financial security of US consumers.

¹ [https://www.regulations.gov/comment/CFPB-2021-0017-0079](https://www.regulations.gov/comment/CFPB-2021-0017-0079)
³ We also believe that the Bureau’s request for comments concerning potential abuse of terms of service and use of penalties merits discussion. We look forward to additional comments from others.
The build-out of Big Tech payment platforms leveraging their unique capabilities to seamlessly combine social media, entertainment, commerce with sophisticated data-driven contemporary surveillance has transformed traditional financial services concepts. Today’s social media giants are also global consumer financial banking and retail institutions. For example, J.P. Morgan has “built a real-time payments infrastructure” for TikTok’s parent company ByteDance:

“That can be connected to local clearing systems. This allows users, content producers, and influencers to be paid instantaneously and directly into their bank accounts at any day or time. ByteDance has enabled this capability in the U.S. and Europe, meaning it covers approximately one-fifth of TikTok’s 1 billion active users worldwide.”

J.P. Morgan assisted ByteDance to also replace its “host-to-host connectivity with banks, replacing it with application programming interfaces (API) connectivity that allows real-time exchange of data” between ByteDance and Morgan. This allows ByteDance to “track and trace the end-to-end status through the SWIFT network, see and monitor payments, and allow users to check for payments via their TikTok or other ByteDance apps in real time.” Morgan also has “elevated and further future-proofed ByteDance’s cash management through a centralized account structure covering all 15 businesses” through a “virtual account management and liquidity tool.”

Google’s Pay operations also illustrate how distinct digital payment platforms are from previous forms of financial services. Google explains to merchants that by integrating “with Google Wallet [they can] engage with users through location-based notifications, real-time updates” and offers, including encouraging consumers to “add offers from your webpage or app directly to Google wallet.” Google promotes the use of “geofenced notifications to drive engagement” with its Pay and Wallet services as well. Google’s ability to leverage its geolocation and other granular tracking and making that information available through a package of surveillance and engagement tools to merchants to drive financial transactions in real-time is beyond the ability of a consumer to effectively address. A further issue is the growing use of “personalization” technologies to make the financial services offering even more compelling. Google has already launched its “Spot” service to deliver “payment enabled experiences for users, including “fully customized experiences” in Google Pay. Although currently available only in India and Singapore, Google’s Spot platform, which allows consumers with “a few simple taps…to search, review, choose and pay” for a product is an example of how payment services online are continually advanced—and require independent review by consumer financial regulators. It also reflects another problem regarding protecting the financial well-being of US consumers. What are the impacts to financial security when there is no distance—no time to reflect—when the seamless, machine and socially-driven marketing and payment operations are at work?

A good example of the lack of meaningful protections for online financial consumers is Google Pay’s use of what’s known as “discovery,” a popular digital marketing concept meaning to give enhanced prominence to a product or service. Here’s how Google describes how that concept works in its Spot-enabled Pay application:

---

5 https://www.jpmorgan.com/content/dam/jpm/treasury-services/documents/case-study-byteance.pdf
“We understand that discovery is where it starts, but building deep connections is what matters the most - a connection that doesn’t just end with a payment, but extends to effective post sale engagement. The Spot Platform helps merchants own this relationship by providing a conversational framework, so that order updates, offers, and recommendations can easily be surfaced to the customer. This is powered by our Order API which is specialised to surface updates and relevant actions for users' purchases, and the Messaging API which can surface relevant messages post checkout to the user.”

Meta (Facebook), along with ad giant WPP, also relies on the growing use of “discovery” applications to promote sales. In a recent report, they explain that “digital loyalty is driven by seamless shopping experiences, convenience, easy discovery, consistent availability, positive community endorsement and personal connections.”

Since Google and other payment platforms have relationships with dozens of financial institutions, and also have an array of different requirements for vendors and developers, USPIRG and CDD are concerned that consumers are placed at a serious disadvantage when it comes to protecting their interests and also seeking redress for complaints. The chain of digital payment services relationships, including with partners that conduct their own powerful data driven marketing systems, requires Bureau review. For example, PayPal is a partner with Google Pay, while the PayPal Commerce Platform has Salesforce as one of many partners.

See also PIRG’s recent comments to the FTC, for an extensive discussion of retail media networks and data clean rooms:

“Clean rooms are data platforms that allow companies to share first party data with one another without giving the other party full access to the underlying, user-level data. This ability to set controls on who has access to granular information about consumers is the primary reason that data clean rooms are able to subvert current privacy regulations.”

**Another important issue for the Bureau is the ability of the Big Tech payment platforms to collect and analyze data in ways that allow it to identify unique ways to influence consumer spending behaviors.** In a recent report, Chinese ecommerce platform Alibaba explained how such a system operates:

“The strength of Alibaba’s platforms allows a birds-eye view of consumer preferences, which is combined with an ecosystem of tactical solutions, to enable merchants to engage directly and co-create with consumers and source suppliers to test, adapt, develop, and launch cutting-edge

---

8 https://developers.google.com/pay/spot
products...helps merchants identify new channels and strategies to tap into the Chinese market by using precise market analysis, real-time consumer insights, and product concept testing.”

**Such financial insights are part of what digital payment and platform services provide.** PayPal, for example, gathers data on consumers as part of their “shopping journey.” In one case study for travel, PayPal explained that its campaign for Expedia involved pulling “together data-driven destination insights, creative messaging and strategic placements throughout the travel shoppers’ journey.” This included a “social media integration that drove users to a campaign landing page” powered by “data to win.” This data included what is the growing use of what’s euphemistically called “first-party data” from consumers, where there has been alleged permission to use it to target an individual. Few consumers will ever review—or have the ability to influence—the PayPal engine that is designed for merchants to “shape [their] customer journey from acquisition to retention.” This includes applications that add “flexible payment options...right on product pages or through emails;” “relevant Pay Later offer to customers with dynamic messaging;” ability to “increase average order value” through “proprietary payment methods;” or “propose rewards as a payment option to help inspire loyalty.”

The impact of data-driven fostered social commerce on promoting the use of consumer payments should be assessed. For example, Shopify’s “in-app shopping experience on TikTok” claims that the placement of its “shopping tabs” by vendors on posts, profiles and product catalogs unleashes “organic discovery.” This creates “a mini-storefront that links directly to their online store for check out.” A TikTok executive explains how the use of today’s digital payment services are distinct—“rooted in discovery, connection, and entertainment, creating unparalleled opportunities for brands to capture consumers’ attention...that drives [them] directly to the digital point of purchase.” TikTok also has partnered with Stripe, helping it “become much more integrated with the world of payments and fintech.”

TikTok’s Stripe integrations enable “sellers to send fans directly from TikTok videos, ads, and shopping tabs on their profiles to products available in their existing Square Online store, providing a streamlined shopping experience that retains the look and feel of their personal brand.” The Square/TikTok payment alliance illustrates the role that data driven commercial surveillance marketing plays in payment operations, such as the use of the “TikTok pixel” and “advanced matching.” In China, ByteDance’s payment services reflects its growing ability to leverage its mass customer data capture for social media driven marketing and financial services.

---

We urge the Bureau to examine TikTok’s data and marketing practices as it transfers U.S. user information to servers in the U.S., the so-called “Project Texas,” to identify how “sensitive” data may be part of its financial services offerings.19

Apple’s payment services deserve further scrutiny as its reintroduces its role as a digital advertising network, leveraging its dominant position in the mobile and app markets.20 PayPal recently announced that it will be “working with Apple to enhance offerings for PayPal and Venmo merchants and consumers.” Apple is also making its payment service available through additional vendors, including the giant Kroger grocery store chain stores in California.21

Amazon announced in October 2022 that Venmo was now an official payment service, where users could, during checkout, “select “Select a payment method” and then “Add a Venmo account.” This will redirect them to the Venmo app, where they can complete the authentication. Users can also choose Venmo to be their default payment method for Amazon purchases on that screen.”22 Amazon’s AWS partners with fintech provider Plaid, another example of far-reaching partnerships restructuring the consumer financial services market.23

Conclusion

USPIRG and CDD hope that both our original comments and these additional comments help the Bureau to understand the impact of rapid changes in Big Tech’s payments network relationships and partnerships. We believe urgent CFPB action is needed to protect consumers from the threat of Big Tech’s continued efforts to breach the important wall separating banking and commerce and to ensure that all players in the financial marketplace follow all the rules. Please contact us with additional questions.

Sincerely yours,

Jeff Chester, Executive Director, Center for Digital Democracy [jeff <at> democraticmedia <dot> org]

Edmund Mierzwinski, Senior Director, Federal Consumer Program, U.S. PIRG [edm <at> pирg <dot> org]

19 https://www.chinadaily.com.cn/a/202211/16/WS6374e81ea31049175432a1d8.html
22 https://techcrunch.com/2022/10/25/amazon-now-allows-customers-to-make-payments-through-venmo/