December 7, 2022

Via Electronic Mail

Comment Intake – Statement into Big Tech Payment Platforms
Consumer Financial Protection Bureau
1700 G Street, NW
Washington, DC 20552
Re: Docket No. CFPB-2021-0017
BigTechPaymentsInquiry@cfpb.gov

Re: Response to Docket No. CFPB-2021-0017 Regarding the CFPB's Inquiry Into Big Tech Payment Platforms

To Whom It May Concern:

The American Bankers Association (ABA),[1] the Consumer Bankers Association (CBA),[2] and the Credit Union National Association (CUNA)[3] appreciate the opportunity to submit comments to the Consumer Financial Protection Bureau (CFPB) in response to CFPB's notice and request for additional comments regarding CFPB's inquiry into big tech payment platforms.[4] As we have previously stressed, and recent crypto events demonstrate, consumers can face appreciable risks when underregulated nonfinancial companies achieve significant scale as *de facto* financial intermediaries, including for payments.

Our members believe that regulators must move beyond monitoring nonbank payments markets and toward action that ensures nonbank payments do not develop into full-fledged shadow banking. A series of actions by CFPB indicate that the agency is accelerating its scrutiny.[5] Last month, CFPB published a final rule amending its procedural rule on supervision of nonbank

[1] The American Bankers Association is the voice of the nation's $23.3 trillion banking industry, which is composed of small, regional, and large banks that together employ more than 2 million people, safeguard $19.2 trillion in deposits and extend nearly $11 trillion in loans.

[2] CBA is the only national trade association focused exclusively on retail banking. Established in 1919, the association is a leading voice in the banking industry and Washington, representing members who employ nearly two million Americans, extend roughly $3 trillion in consumer loans, and provide $270 billion in small business loans.

[3] Credit Union National Association (CUNA) is the only national association that advocates on behalf of all of America's credit unions, which are owned by 130 million consumer members. CUNA, along with its network of affiliated state credit union leagues, delivers unwavering advocacy, continuous professional growth, and operational confidence to protect the best interests of all credit unions.

[4] "Notice and Request for Comment Regarding the CFPB's Inquiry Into Big Tech Payment Platforms," 87 Fed. Reg. 67,023 (Nov. 7, 2022).

[5] "Supervisory Authority Over Certain Nonbank Covered Persons Based on Risk Determination," 87 Fed. Reg. 70,703 (Nov. 21, 2022); 12 C.F.R. pt. 1091.

entities based on risk factors and additionally has commenced its rulemaking on personal financial data rights, which necessarily will include nonbank participants in the ecosystem. We urge CFPB to continue to increase its oversight until all consumers are protected at a consistent level, no matter the legal structure of the entity.

One year ago, ABA, CBA and CUNA applauded CFPB's initial inquiry into the payment platforms of the largest information technology companies (big techs) as an urgently needed step forward in the federal government's oversight of increasingly powerful nonbank payments providers.[6] The comment record is clear evidence of widespread concern from members of the public about how big tech entities are positioned to use their scale and other advantages to pursue relentless collection, accumulation, and monetization of personal data, and other advantages made possible only through their nonfinancial products.

America's payments system, built in large part by banks, is competitive, increasingly fast, and affordable. Paying with your bank or credit union is easy and getting easier. It is also becoming safer and less expensive. Bank and credit union payments provide unparalleled value to all parties in the ecosystem. Our members are in payments for the *business of payments* and understand the need to provide consumer protection, privacy, and data security; contrariwise, big tech is getting into payments to buttress their other core businesses, and to obtain access to more data about the lives of Americans.

The financial services industry's payments agenda is simple: strong consumer protection, fair and consistent rules, funds that are safe and secure, and transactions paid through fair pricing rather than by the selling of consumer data. As shared last year, ABA, CBA, and CUNA support CFPB's focused efforts to prevent regulatory arbitrage and the exploitation of consumers and their information by big techs that are attempting to capture the most valuable parts of the payments chain for themselves rather than building inclusive ecosystems for all. To that end, CFPB should ensure potential consumer protections are applied consistently to all companies offering payments products and financial services, including big techs.

* * * *

Big Tech's Growing Ambitions in Payments

Big tech possesses fundamental advantages in expanding their payments activities. A 2022 Congressional Research Service (CRS) report noted that, "[i]rrespective of the nature of their relationships and current role in financial intermediation, Big Tech companies have demonstrated interest and possess the scale and financial capacity to increase their range of offerings of financial products should they choose to do so. Traditional economic factors such as economies of scale and network effects—and the unique advantages of the Big Tech business model, which relies on access to troves of data and insight into consumers' behavioral preferences—support this reality."[7]

---

[6] CBA and ABA, *Response to Docket No. CFPB-2021-0017 Regarding the CFPB's Inquiry Into Big Tech Payment Platforms* (Dec. 6, 2021), *available at* https://www.consumerbankers.com/sites/default/files/CBA%20and%20ABA%20Joint%20Trades%20Letter%20--%20Comment%20to%20Docket%20No.%20CFPB-2021-0017.pdf.

[7] "Big Tech in Financial Services," Congressional Research Service (July 29, 2022).

For big tech platforms that redefined entire markets, from photo sharing to news, payments have proven to be the next target for expansion. Be it Twitter's reported interest in starting a payments platform or other firms' investments in fintechs, big tech interest in payments endures. In some instances, it appeared that firms assumed that merely being a tech company (or *not a bank*) carried with it special privileges or regulatory deference to experiment without the usual obligations that protect consumers and the financial system itself. This is the opposite of the impression these companies should have, and we hope that CFPB will clarify that this mistaken presumption is incorrect. Because they are less regulated than banks and, further, lack institutional knowledge of the risk environment, big techs should receive very robust scrutiny and consideration of their greater risk profiles.

We encourage CFPB to solidify its current efforts into a permanent oversight infrastructure for nonbank participants in the payments business. Not only will these entities be on notice that there is a "cop on the beat," but the knowledge that their future products will operate under the watchful eye of regulators will guide their product roadmaps. Preventing negative events in the payments marketplace is critical to avoid consumer harm. This is not a time-limited project, but an enduring and fundamental mission of the CFPB.

Buy Now Pay Later as an Example of Shadow Payments

The financial services industry, and our associations, were early in identifying the risk that unregulated Buy Now Pay Later (BNPL) firms would pose to consumers. Based on their clear history abroad of providing products that overwhelmed underqualified borrowers and produced chronically poor consumer outcomes, we urged CFPB to consider appropriate measures to ensure BNPL products continue to be accessible to consumers to meet their financial needs while ensuring that consumers receive the same disclosures and protections they are accustomed to, regardless of whether the product is offered by a bank/credit union or nonbank. While there is still more work to be done and oversight should continue, CFPB effectively surveyed the market and appropriately acted. In many ways, the growth and harms associated with BNPL mirror those of big tech's role in payments.

There are parallels between the BNPL experience and what could lay ahead for underregulated big tech consumer financial services.

While the BNPL concept can be responsibly offered and there are signs of reforms in the industry, it reached scale quickly, even without the benefit of the network effects that big tech brings. Through integration with trusted merchant brands, many of which were willing to pay higher payment acceptance costs than they pay for credit cards, consumers assumed nonbank BNPL loans were safe options. Similarly, big tech may create the impression for consumers that their experience in social networking or another service within their realm of acknowledged competence extends to payments, which is a vastly different product. It is not readily apparent to consumers at the checkout selecting a payment option from a big tech entity that the consumer is not transacting with a financial services company (like a bank or credit union) that has an extensive compliance program coupled with privacy and security protections. With the vast network of these companies' platforms, this consumer exposure could scale rapidly.

Consumer Privacy, Data, and Section 1033

A full treatment of Dodd-Frank Act Section 1033 is beyond the scope of this letter. However, as CFPB works toward finalizing a Section 1033 rule, we encourage the agency to be aware of the ways in which big techs could exploit the regulation to push consumers into giving consent for financial information sharing. Perhaps no other regulatory vehicle on the horizon could so empower big tech, if the final rule fails to take into account the realities of the marketplace and the incentives for nonbank payments firms to use every tool available to quickly scale up. As an example, if the updated terms of use for a big tech's userbase are amended to include consent for the company to receive the consumer's financial data, many consumers could be simultaneously added onto a nonbank financial network. In some respects, there would be virtually no meaning to that consent. Until recent developments in data aggregation, consumers have known with certainty when they are providing payment credentials to a merchant; for instance, by physically keying in a credit card number or selecting a card from a digital wallet. The ability of big tech firms to directly and continuously access consumers' deposit accounts blurs consent in a way that could create confusion, at the least, to say nothing of the downstream uses of that data. The potential enmeshment of big tech with the most sensitive financial details of consumers is a prospect which should concern CFPB and other financial regulators.

We believe CFPB should ensure that data users that are larger participants in the financial services or aggregation services market – not just banks and credit unions – are examined for compliance with applicable federal consumer financial law, including the substantive prohibitions on the protection, permissible use, and release of confidential consumer information.

Fees and Fines on Platforms and Incentives in Payments Systems

As CFPB looks into the questions added for this reopened docket regarding fines and penalties related to acceptable use of payments products, we encourage CFPB to avoid conflating this targeted nonbank conduct with the legal, fair, and necessary practices of financial institutions, including the execution of chargebacks to settle merchant-consumer disputes and penalties for businesses' non-compliance with data security obligations. These form the basis of the incentives, trust, and accountability within multi-party payments systems, such as card systems.

The events and concerns that precipitated the reopening of this docket are completely distinct from the fees that may arise as the financial services industry attempts to safeguard the payments system and protect financial data. Adherence to strong data protection requirements is foundational to a safe, functioning payments system. As a practical example, when a financial institution's customers face fraud or inconvenience due to a merchant data breach, there are circumstances where the merchant's culpability rises to the level where the bank or credit union is compensated a modest amount to offset the cost of reissuing cards and resolving their customers' situations. These processes are particularly important to small community financial institutions that must remediate damage caused by the failures of often-large retail firms to safeguard payments data. Interfering with the ability to enforce compliance with these pro-consumer baseline expectations would have unpredictable results.

Conclusion

We appreciate the opportunity to comment once again on this important fact-finding docket by CFPB. Innovation and competition are integral to the marketplace, but must be undertaken responsibly; accordingly, all participants and products in that market need to be subject to uniform and appropriate safeguards that protect consumers.

Sincerely,

AMERICAN BANKERS ASSOCIATION

CONSUMER BANKERS ASSOCIATION

CREDIT UNION NATIONAL ASSOCIATION