December 6, 2021

Via Electronic Submission

Comment Intake-Statement into Big Tech Payment Platforms
Bureau of Consumer Financial Protection
1700 G Street NW
Washington, DC 20552

RE: Notice and Request for Comment Regarding the CFPB's Inquiry Into Big Tech Payment Platforms [Docket No. CFPB–2021–0017]

Dear Sir or Madam:

The Independent Community Bankers of America ("ICBA")[1] welcomes this opportunity to comment on the Bureau of Consumer Financial Protection's ("CFPB" or "The Bureau") concerns regarding big tech payment platforms ("big tech"). ICBA and its members appreciate the CFPB's inquiries into the role these companies play in the broader payments and financial services ecosystem. The safety and protection of consumers' financial data should be a top priority for all parties wishing to participate in the industry.

As noted, technological innovation and deployment continues to alter the way that consumers and businesses conduct banking and commerce and influences the products that community banks offer. The benefits that big tech offers to consumers and small business can be quite valuable. However, as was pointed out, technology companies wield great power and influence over the market with limited incentive to ethically manage consumer financial data. Similar to the examination and oversight authority prudential regulators have on the financial industry, regulators must play an equally active role in defining and identifying the risks big tech poses to consumers and businesses alike.

[1]*The Independent Community Bankers of America® creates and promotes an environment where community banks flourish. ICBA is dedicated exclusively to representing the interests of the community banking industry and its membership through effective advocacy, best-in-class education, and high-quality products and services. With nearly 50,000 locations nationwide, community banks constitute 99 percent of all banks, employ more than 700,000 Americans and are the only physical banking presence in one in three U.S. counties. Holding more than $5.7 trillion in assets, over $4.7 trillion in deposits, and more than $3.6 trillion in loans to consumers, small businesses and the agricultural community, community banks channel local deposits into the Main Streets and neighborhoods they serve, spurring job creation, fostering innovation and fueling their customers' dreams in communities throughout America. For more information, visit ICBA's website at www.icba.org.*

Protection of consumer financial data is paramount to the integrity of the financial services sector. All participants in the broader payments and financial sector ecosystem should be subject to Gramm-Leach-Bliley Act ("GLBA") like data security and privacy standards to protect consumer data where it exists.

Summary

Technology companies, large and small, have dramatically increased their presence in the financial services sector in recent years. ICBA acknowledges that technology companies play a vital role in the financial lives of consumers and small businesses, both providing unique services and enabling community banks to provide their customers with the latest cutting-edge financial technology. However, the value added must be weighed against the risks big tech poses both to consumers and to the integrity of the broader financial services industry. ICBA urges the CFPB to continue exploring and studying the practices of not only big tech payments companies, but of all technology companies participating in payments and financial services, or that hold consumer data.

Non-bank entities, namely large technology companies and data aggregators, benefit from unregulated access to and storage of sensitive consumer financial data without the scrutiny of examinations. The integrity of consumer data and privacy is only as strong as the weakest link protecting that information, and as more non-regulated entities handle consumer data, the risk of breach and/or loss increases. Under current federal law, technology companies and other parties that process or store consumer financial data are not subject to the same federal data security standards and oversight as financial institutions. Non-bank entities obtaining, holding, or otherwise using consumer financial data must be held responsible for ensuring the security of the consumer information they possess and must be held liable for any data breaches and consumer harm as a result of handling such data.

Additionally, technology companies are continuously looking to increase their presence in the financial services ecosystem, with the end goal of offering the full-service banking services through FDIC-insured industrial loan companies ("ILCs") and avoiding oversight and regulation under the Bank Holding Company Act. One of the companies subject to the CFPB order has already received an ILC charter. If these technology companies gain ownership over ILCs, the privacy concerns, the anti-competition concerns, and the general market exploitation concerns the Bureau expressed in its statement will be dramatically worsened.

As the CFPB continues to look into the practices of big tech companies, ICBA urges the following:

- Do not limit examinations to big tech payment platforms but also consider data aggregators and other entities which handle, store, and use consumer financial data.
- Ensure all companies participating in the payments and financial services ecosystem are held to GLBA-like data security standards to properly secure consumer financial data.
- Hold breached companies liable for the costs of making consumers whole.
- Work with regulators to ensure that the ILC loophole in the Bank Holding Company Act is not abused by technology companies.
- Require data minimization standards for technology companies accessing consumer financial data.

ICBA's Comments

Do Not Limit Inquiry to Big Tech

ICBA commends the Bureau's initial order directed at six of the largest technology companies offering payment services. There is much to learn and understand about their data practices that will help to ensure a safer payments and financial services ecosystem.

The Bureau's order to examine the practices of six of the largest technology companies is a good first step toward ensuring consumer safeguards. However, ICBA urges the Bureau to expand its inquiry to data aggregators. Data aggregators play a large role in the procurement and usage of consumer financial data. Data aggregators serve as middlemen between millions of consumers and thousands of financial technology companies, collecting data on consumers who wish to use websites or applications that have agreements with the data aggregators.

The amount of data to which data aggregators have access is staggering. For example, one data aggregator states that 25% of all people in the U.S. with a bank account have connected to their company.[2] While the aggregators pass along the data required to make the application work to the technology company, they also store any other permissioned data. Depending on how these accounts were permissioned, an aggregator may have complete access to a consumer's account and account data via screen scraping. Furthermore, most consumers do not understand that they have permissioned the data aggregator - in addition to the application or company - to obtain their account data.

[2] https://www.cnbc.com/2020/01/13/visa-to-acquire-plaid-the-fintech-powering-venmo-and-other-banking-apps-for-5point3-billion.html

Data aggregators, as well as big techs, benefit from unregulated access to this sensitive consumer financial data without the oversight of examinations. Banks, on the other hand, are vigorously examined by various federal regulators for consumer and data protection compliance. As aggregators and technology companies continue to collect consumer data without commensurate supervision, the risk of harm to the consumer continues to increase.

ICBA believes that the Bureau should exercise its formal and explicit supervision and enforcement authority over big tech and data aggregators.[3] Given these companies' prolific access to and storage of consumer data, the CFPB should supervise and examine data aggregators and brokers under its "larger participants" authority under Section 1024 of the Dodd–Frank Wall Street Reform and Consumer Protection Act. This would enable the Bureau to detect and assess risks to consumers and the consumer financial markets as well as ensure compliance with consumer protection laws.

All Entities in the Financial Services Ecosystem Should Be Subject to Strong Data Security Requirements

It is imperative that all participants in the payments and financial sector ecosystem, including aggregators and technology companies with access to customer financial information, should be subject to GLBA-like data security standards.

Community banks are governed by some of the strictest data security laws and regulations set forth by the GLBA and its implementing regulations and Safeguards Rule. These regulations require financial institutions to disclose their information-sharing practices to their customers, provide certain choices to consumers in how the data is used, safeguard sensitive data, and create robust data security. Protecting consumer financial data is central to maintaining public trust and key to long-term customer retention. Community banks are proud of the security they provide and believe existing laws and regulations appropriately mitigate risks to consumer financial data while that data is being held by community banks.

However, not all entities are governed by such strict security regulations. Technology companies holding the same data are not required to have strict data security practices. No matter how securely community banks store consumer data, if others in the ecosystem are not required to have similar safeguards, consumer data will be at higher risk.

[3] 77 Fed Reg 42873 (07/20/2012). https://www.federalregister.gov/documents/2012/07/20/2012-17603/defining-larger-participants-of-the-consumer-reporting-market

Liability and Costs for Consumer Harm Must Be Borne by the Breached Party
When a breach occurs at a nonbank entity holding consumer financial data, community banks are too often left to mitigate the damage done to consumers. The following are examples of the disproportionate costs and burdens placed on community banks when nonbank entities incur a breach.

- In 2014, when Home Depot was breached, community banks were responsible for replacing payment cards, notifying customers of the breach, implementing enhanced monitoring of accounts, and reimbursing customers for fraudulent transactions.[4]
- In 2017, when Equifax was breached and sensitive personal information of millions of consumers was stolen, community banks faced untold damages due to the unique circumstances of the massive data breach.[5] At their own cost community banks instituted additional protective measures to deter customer identity theft and fraudulent transactions. Additionally, community banks bore the responsibility for costs associated with payment card cancellation and replacement, fraudulent charges, customer notification, and closing affected accounts, all while monitoring the risk of exchanging information with Equifax.
- In 2021, when Costco experienced the use of debit and credit card skimmers at their point-of-sale terminals, community banks were responsible for replacing payment cards and reimbursing customers for fraudulent transactions.[6]

While these incidents vary considerably in attack type and complexity, one constant remains true throughout – non-bank entities must have the same stringent protections in place as financial institutions. This will protect consumer data and hold entities accountable for the full cost of making consumers whole instead of shifting that cost to banks. ICBA urges the Bureau to hold all entities who handle consumer financial data to similar data security standards to which financial institutions are held.

Big Tech Seeks Additional Market Power
Big tech's foray into the payments landscape skates dangerously close to the desire shown by many large corporations to form Industrial Loan Companies ("ILCs").[7] In today's digital economy, the desire for big tech to participate in financial services without the commensurate oversight and regulation[8] creates a myriad of risks, not only to consumers' financial privacy, but to economy as a whole.

---

[4] https://ir.homedepot.com/news-releases/2014/11-06-2014-014517315
[5] https://www.equifaxsecurity2017.com/updates//-/announcements/a-progress-update-for-consumers
[6] https://www.documentcloud.org/documents/21103155-costco_data_breach_notification_bc_card_skimmer_device
[7] For additional information about threat and systemic harm ILCs pose, please reference ICBA's 2019 white paper on ILCs: https://www.icba.org/docs/default-source/icba/advocacy-documents/reports/ilc-white-paper.pdf
[8] A loophole exists in the Bank Holding Company Act that allows commercial companies to own FDIC insured ILCs without Federal Reserve oversight of the holding company or limitations on non-banking activities that are designed to promote safety and soundness and guard against conflicts of interest, concentration of economic power, and undue harm to consumers and competition.

WASHINGTON, DC
1615 L Street NW
Suite 900
Washington, DC 20036

SAUK CENTRE, MN
518 Lincoln Road
P.O. Box 267
Sauk Centre, MN 56378

866-843-4222
www.icba.org

Payments platforms are certainly only the beginning of big tech's financial services goals. In recent years, there have been ILC applications from technology companies such as Square and SoFi, as well as mega-retailors Walmart and Home Depot. With social media companies and other big tech/big data companies beginning to offer financial products and services, a small number of companies could hold tremendous market power. The integration of these technology and banking firms would pose conflicts of interest and privacy concerns to our banking system. What will happen when big tech extends their reach into our financial lives?

Today, these companies already track our movements, our friends, our families and associates, our religious and political affiliations and views, our internet browsing, and our shopping history. Adding personal, financial data would take their capabilities to a new level. Not only would a technology company in control of an ILC be able to dictate who receives loans, potentially cutting off access to credit to competitors, but they would dramatically change the competitive landscape of the U.S. economy as a whole, removing the neutrality traditional banks bring to the provision of credit.

ICBA is concerned about the potential market power and market manipulation which may occur as more technology companies attempt to enter the financial services industry.

Financial Technology Companies Should Practice Data Minimization

To address concerns regarding the amount of data to which technology companies and data aggregators have access, ICBA strongly supports limiting the use, sharing, and storing of data by financial technology companies to that which is explicitly authorized by the consumer. In a similar vein to data access control with zero trust,[9] data for which the consumer has authorized access should have limited application functionality, providing only minimal access, collection, use and storage for a restricted period of time. Technology companies wishing to participate in financial services must not be allowed to aggregate, hold, and manipulate data in ways which may impact a consumer's access to financial products. Limiting the amount of data these companies have access helps mitigate consumer risks in the event of a breach or misuse of data. These restrictions should also apply to limiting data to the original entity receiving permission. The sale or sharing of data to unpermissioned third parties should be prohibited.

Conclusion

ICBA thanks Director Chopra and the Bureau for the opportunity to comment on this very important issue. The safety and security of consumer financial data is paramount to the integrity of the financial services industry and the protection of consumer information. While community

[9] Per NIST: "Zero trust is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated…The initial focus should be on restricting resources to those with a need to access and grant only the minimum privileges needed to perform the mission." https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

banks pride themselves on creating a trusted secure environment, all participants in the industry must abide by the same standards.

If you have any questions, please do not hesitate to contact me at Steven.Estep@icba.org or (202)-821-4329.

Sincerely,

/s/

Steven Estep
Assistant Vice President, Operational Risk