December 10, 2021

*Via Electronic Mail*

Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552
Attn: Comment Intake

Re: Notice and Request for Comment Regarding the CFPB's Inquiry Into Big Tech Payment Platforms (Docket No. CFPB–2021–0017)

Ladies and Gentlemen:

The Bank Policy Institute[1] appreciates the opportunity to comment on the Notice and Request for Comment Regarding the Inquiry Into Big Tech Payment Platforms ("Notice")[2] issued by the Consumer Financial Protection Bureau ("CFPB" or "Bureau"). BPI supports innovation and welcomes competition in payments and other activities in which banks engage when this innovation is conducted responsibly and in a way that ensures that customers are protected through consistent regulation and oversight. However, both customers and the U.S. financial system are put at risk when Big Techs and fintechs[3] offer banking products and services without adhering to all the consumer regulatory protections banking organizations are required to follow and with far more limited – if any – onsite supervision to determine compliance with those regulations.

In recent years, tech companies have unbundled traditional banking services, such as deposit-taking, payments, and lending activities, and offered one or more of these products, or access to these products, to consumers outside of the ordinary federal bank regulatory perimeter. Tech companies have been able to grow at exponential rates, attracting millions of customers while simultaneously avoiding both the robust regulatory, supervisory, and examination regime that applies to ordinary banks and the longstanding U.S. prohibition on mixing banking and commerce. In short, these tech companies are able to provide products and services that may be perceived by customers as equivalent to those provided by banks, while avoiding the framework put in place by Congress and federal banking regulators to ensure that consumers are protected and the overall financial system remains safe, sound and stable.

---

1 The Bank Policy Institute is a nonpartisan public policy, research, and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost 2 million Americans, make nearly half of the nation's small business loans, and are an engine for financial innovation and economic growth.

2 Notice and Request for Comment Regarding the CFPB's Inquiry Into Big Tech Payment Platforms, 86 Fed. Reg. 61182 (November 5, 2021).

3 Hereinafter, the term "tech companies" is used to refer to Big Tech and fintech companies.

In light of the risks to consumers presented by tech companies' offering payments services outside of the federal bank regulatory regime, the CFPB should ensure that consumers and their personal financial data are protected when using those companies' payments services. In addition, the CFPB should coordinate with other regulators and policymakers to ensure that tech companies and other nonbank providers are subject to a regulatory, supervisory, and examination framework designed to protect consumers and the safety and soundness of the financial system.

## I. Consumers Should Not Sacrifice Critical Protections When Using Tech Payments Platforms.

It is critical that consumers are afforded the same level of protection whether they obtain banking services from a traditional bank or a tech company. Banks are subject to supervision and regular examination for compliance with a host of consumer protection laws and regulations, including fair lending laws, such as the Equal Credit Opportunity Act, and laws prohibiting Unfair, Deceptive, and Abusive Acts and Practices, anti-steering requirements, and the Electronic Funds Transfer Act. While tech companies operating payments platforms are today subject to certain consumer protection requirements, some tech companies "make technical, and questionable, arguments that their products or services fall outside the existing regulatory framework."[4]

Further, those companies "are not subject to the same type of regular, direct supervision as banks, and the enforcement authority for applicable consumer protection requirements on fintech activities is scattered among various federal and state regulators," creating "an unfair business advantage . . ."[5] In addition, the diffuse organizational structure of many tech companies raises questions about who is responsible for consumer compliance and the mechanisms in place to ensure that those protections are implemented. Banks, in contrast, have significant experience and expertise in implementing consumer protection safeguards. In addition, banks are subject to regular consumer compliance examinations to further assure consumers that the bank is appropriately managing its consumer compliance function.

Another concern arises from many tech companies' massive stores of non-financial but personal data about many aspects of their users' lives and the opacity surrounding the collection and certain uses of that data.[6] Tech companies are in the business of building large networks of users and capturing those users' data.[7] It is essential that tech companies' accumulation of financial data from their payments businesses, combined with customers' non-financial data obtained from their other, primary businesses, be subject to the consumer protections that result from appropriate supervision, including compliance with informed consent and permissible use restrictions, proper disclosure about use, model

---

4 *See* Acting Comptroller Michael J. Hsu, Remarks before the American Fintech Council Fintech Policy Summit 2021, "Leveling Up Banking and Finance" (November 3, 2021) at 7, *available at*: Acting Comptroller Michael J. Hsu Remarks before the American Fintech Council Fintech Policy Summit 2021_Leveling Up Banking and Finance (occ.gov).

5 *Id*.

6 See, e.g., Bank for International Settlements "Annual Economic Report, Big tech in finance: opportunities and risks" (June 23, 2019) at 67-8, available at: III. Big tech in finance: opportunities and risks (bis.org) ("Another, newer type of risk is the anticompetitive use of data. Given their scale and technology, big techs have the ability to collect massive amounts of data at near zero cost. This gives rise to "digital monopolies" or "data-opolies". Once their dominant position in data is established, big techs can engage in price discrimination and extract rents. They may use their data not only to assess a potential borrower's creditworthiness, but also to identify the highest rate the borrower would be willing to pay for a loan or the highest premium a client would pay for insurance . . . ") (internal citations omitted).

7 *Id*.

governance and fair lending rules.[8] For example, unless explicitly permissible by applicable law or regulation, a non-financial affiliate providing an e-commerce platform linking customers and merchants should be prohibited from using data or insights obtained from customer payment activity to market or price any other product or service targeting such customer.

Banks, of course, also use consumer data and related innovations for various aspects of their businesses, including models developed from their data. However, banks engage in significant testing to ensure that their use of data and models does not inadvertently result in consumer harm – for example, by inadvertently discriminating against certain classes of customers. In addition, banks are subject to direct and robust consumer compliance supervision and examination, including in connection with their use of data and models, which serves as an additional layer of protection for consumers. Tech companies do not face any comparable checks on their use of data or models, which could result in consumer harm, especially in light of the massive stores of data amassed by many of these technology companies. Consistent standards should apply to the collection and use of consumer data across banks and nonbanks. Comparable operational resilience requirements would also support these goals.

Finally, in contrast to banks, which invest significant time and money in developing robust customer support departments to help customers troubleshoot any issues that may arise with the bank's products and services, the diffuse structure of tech companies may significantly impair a customer's ability to obtain assistance or support from the company for a wide range of questions or issues.

The CFPB possesses a variety of tools to protect consumers from harm. Pursuant to Section 1024 of the Dodd-Frank Act, the CFPB has authority over "any covered person who… is a larger participant of a market for other consumer financial products or services, as defined by rule …."[9] To date, the CFPB has defined "larger participants" in the consumer reporting, consumer debt collection, student loan servicing, international money transfer, and automobile financing markets, which has allowed the agency to examine the activities of these larger participants in a similar manner to those covered persons routinely supervised by the CFPB pursuant to Section 1025.[10] BPI recommends that the CFPB use its authority under Section 1024 to designate for coverage larger participants in the domestic electronic payments market. In light of the exponential growth of tech companies in the payments market and the risks to consumers presented by these companies' participation in this market, engaging in such a rulemaking to bring greater oversight to those companies would help to protect consumers.

## II. Tech Companies Must Provide Strong Security and Consent Protections to Consumer Data, Just as Banks Do

Tech companies' payments platforms raise significant privacy and data protection issues for consumers. While banks are subject to a variety of requirements as well as supervision and examination regarding the protection of consumer data, including the Gramm-Leach Bliley Act (GLBA), tech companies are not subject to this same oversight. GLBA requires financial institutions to disclose their information-sharing practices, offers consumers the right to opt-out of certain sharing, and implements reasonable policies and procedures for data safeguarding. Customer financial data that would be

8 *Id*.

9 12 U.S.C. § 5514(a)(1)(B).

10 12 C.F.R. Part 1090.

protected in the hands of a regulated financial institution should not be subject to less robust oversight when it is acquired or held (by any means) by a technology firm seeking to offer financial service alternatives. While some tech companies are subject to the FTC safeguards rule, which implements certain requirements set forth in GLBA, the FTC does not have supervisory or examination authority over those entities and can thus initiate enforcement actions only after some wrongdoing has occurred and is discovered. Ex ante supervision and examination serves to help prevent consumer and other harm from occurring in the first place. Although tech companies are subject to supervision and examination by the various states in which they are licensed, the data protection requirements accorded to customers vary by state. The CFPB and other policymakers should ensure that tech companies are subject to sufficient oversight to ensure that consumer data collected in connection with a consumer financial service or transaction is protected consistent with the requirements that apply to regulated banks, including those set forth in GLBA. The FFIEC examination guidance on information security also could serve as a useful model for the Bureau in developing the appropriate information security standards for tech companies.[11]

In addition, informed consumer consent should be required before tech companies or other data users access, use, or share consumer data.[12] To enable the functionality of tech payments platforms, consumers often agree to share their banking credentials with data aggregators that link customers with the platform. Some tech companies collect other, non-financial data in connection with financial transactions or deploy non-financial data obtained through other services to market and operate their financial services. Some tech companies allow consumers to use their user credentials to access financial services offered by other companies, thereby gaining insight into the customers' utilization of other companies' products and services. Consumers often do not fully understand for what purposes and for how long their data can be used. The terms of service often allow technology platforms and other third-parties to use and monetize customer data generated in ways customers may not have envisioned and for periods longer than necessary.[13]

Consumers should have full awareness and control over how their data is obtained, shared and used. To that end, consumers should be made aware of the accounts and data that will be accessed by third-party data users. Consumers cannot make informed choices without transparent and readily accessible and understandable disclosures. As the CFPB stated in its principles for consumer-authorized financial data sharing, firms seeking to obtain consumer authorization for sharing their financial data

---

11 FFIEC, Information Technology Examination Handbook, Information Security Booklet, available at FFIEC IT Examination Handbook InfoBase - Information Security.

12 *See* "Statement by the Bank Policy Institute Before the U.S. House Committee on Financial Services Task Force on Financial Technology "Preserving the Right of Consumers to Access Personal Financial Data" (September 21, 2021), *available at:* Statement by BPI - House FinTech Task Force Consumers to Access Personal Financial Data 2021.09.21; see *also* BPI comment letter responding to the Bureau's Advance Notice of Proposed Rulemaking on Consumer Access to Financial Records (February 4, 2021). *Available at*: BPI-Comment-Letter-Responding-to-CFPB-1033-ANPR-2021.02.04.pdf

13 A December 2021 survey conducted by The Clearing House, a banking association and payments company that supports industry collaboration and development, found that 80% of consumers are largely unaware that apps use third-party providers to gather users' financial data; only 24% know that these data aggregators can sell personal data to other parties for marketing, research, and other purposes; 73% of app users are unaware that fintech apps have access to their bank account username and password even though app users have given that information as part of the sign-up process; and 78% did not know that aggregators regularly access personal data even when the app is closed or deleted. "The Clearing House, 2021 Consumer Survey: Data Privacy and Financial App Usage," (December 2021), *available at*: 2021-TCH-ConsumerSurveyReport_Final (theclearinghouse.org).

should provide clear disclosures regarding the "identity and security of [the] party, the data they access, their use of such data, and the frequency at which they access the data . . . throughout the period that the data are accessed, used, or stored."[14] Consumers must have the ability to consent to share their financial data, the information and ability to understand what they are consenting to, and the ability to confirm, modify and revoke access once granted. As a minimum safeguard, data aggregators and data users should be required to periodically provide updated explanations of the sharing that they engage in, and require consumer re-authorization to access consumer data. Perpetual or long-term access permissions unnecessarily put consumers and their data at risk. At a minimum, data aggregators and data users should be required to obtain the consumer's additional affirmative consent before they are allowed to use the consumer's data for a secondary use not reasonably expected by consumers, thereby empowering consumers to control all the potential uses by permissioned parties of their data. In addition, data minimization is a fundamental security principle: limiting the collection or dissemination of sensitive data reduces the consumer's risk of exposure. Consumers therefore should be able to limit what data a third party can access and the purposes for which the data may be used.[15]

## III. The CFPB Should Coordinate with the Federal Banking Regulators and Other Policymakers to Establish Robust Requirements for Tech Payment Platforms to Ensure the Safety and Soundness of The Financial System.

Tech companies operating payments platforms offer services and products in direct competition with banks, yet they are not subject to the same type of regular, direct supervision. Further, technology firms operating payments platforms often do not limit themselves to storing payment credentials and transaction data. Rather, they frequently provide accounts to store value (money equivalents), enabling technology firms to layer increasingly sophisticated financial service offerings and credit functionalities that rely on the entire customer interaction happening within the app. These "convenience features" often create deep dependencies that make switching unlikely or impracticable, thereby reducing the competitive pressure on the technology firm offering the app.[16] In addition, these stored value offerings may lead to customer confusion about where customer funds sit and whether these funds are FDIC-insured.[17]

---

14 Consumer Financial Protection Bureau, "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation" (Oct. 18, 2017), *available at*: https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf. Principle 2 states that participants should "only access the data necessary to provide the product(s) or service(s) selected by the consumer."

15 *See id*.

16 Antitrust authorities in other jurisdictions are reviewing whether certain apps with embedded finance offerings raise anti-competitive concerns. For example, The Netherlands' Authority for Consumers and Markets in September 2021 found that Apple's rules requiring software developers to use its in-app payment system are anti-competitive and ordered it to make changes. Apple faces similar reviews in other countries, including South Korea. Chee, Foo Yun, Toby Sterling, and Stephen Nellis, "Dutch watchdog finds Apple app store payment rules anti-competitive – sources." *Reuters*, Oct. 7, 2021, *available at*: EXCLUSIVE Dutch watchdog finds Apple app store payment rules anti-competitive - sources | Reuters

17 For example, in many cases, when a customer holds funds in a fintech app wallet, the funds sit on the balance sheet of fintech and may not be FDIC-insured. However, if a customer holds funds on a debit card issued through a partnership with a Durbin-exempt small bank, for example, the funds are covered by the bank's pass-through FDIC insurance. Even where pass-through coverage is available for some funds held through a fintech app or debit card, the operational procedures applicable to some fintech offerings are complex and result in funds passing through one or more accounts where pass-through coverage is not available before coming to rest in an account where it is, making it difficult for customers to know when and how much of their funds are insured.

While these payments platforms purport to only process payments, "[t]oday, with the rebundling of banking by synthetic banking providers [including tech companies], the money held by payments platforms looks less like the spare cash in one's wallet and more like the cash one holds in a bank deposit. At the same time, those platforms are now extending material amounts of credit. On demand, par liabilities mixed with credit risky assets: these are the ingredients that can lead to runs."[18] Thus, these tech companies that operate payments platforms outside of the federal bank regulatory perimeter could impose significant harm on the financial system.

While runs and losses can occur at banks, as noted, the prudential requirements to which banks are subject are designed to mitigate that run risk, particularly under the regulatory framework adopted following the 2007-2008 financial crisis. Payments platforms operating outside of the federal bank regulatory perimeter are not subject to the prudential regulation applicable to banks, including stringent capital and liquidity requirements, nor are they subject to a host of other requirements intended to ensure banks' safety and soundness. Although these payments businesses generally are subject to state money services business licensing requirements and regulation, the mechanisms imposed by the states on money services businesses to protect customers from liquidity and loss of value fall "far short of the high standards set by . . . [the] more sophisticated regulatory frameworks" to which banks are subject.[19] The minimum net worth requirements applicable to money services businesses "typically contemplate a relatively thin layer of protection in comparison with bank capital requirements."[20] Similarly, the surety bond and other security requirements for these businesses fall far short of customer funds in the large payments companies' customer accounts, and further, some of these requirements are fixed amounts or based on the number of physical locations or the volume of payment flows and thus "may not reflect the aggregate size of the positive account balances held by customers within each state."[21] In addition, "many states contemplate the relaxation or removal of these security requirements after the expiry of a specified timeframe."[22] The treatment of these assets in the event of the money transmitter's failure may not be as clear as the treatment of customer deposits held by banks (even leaving deposit insurance aside). Finally, a significant number of states allow these payments businesses to invest in volatile assets, such as corporate debt and publicly traded securities, which could fall in value to less than a payments company's outstanding payment obligations.[23] This volatility could lead to delays in transferring or converting deposited funds and, "[o]nce in insolvency, this volatility also exposes customers to the risk that the value of the firm's investment portfolio will be insufficient to ensure full repayment. ***Viewed in this light, state money transmitter laws are a poor substitute for the legal protections typically enjoyed by bank depositors***."[24]

---

18 Hsu at 6-7.

19 Awrey, Dan, "Bad Money" (February 5, 2020), 106:1 Cornell Law Review 1 (2020); Cornell Legal Studies Research Paper No. 20-38, at 47, *available at*:
SSRN: https://ssrn.com/abstract=3532681 or http://dx.doi.org/10.2139/ssrn.3532681.

20 *Id*. at 48.

21 *Id*. at 51.

22 *Id*.

23 *Id*. at 51-56.

24 Awrey, Dan and van Zwieten, Kristin, "Mapping the Shadow Payment System" (October 8, 2019) at 35 (emphasis added). SWIFT Institute Working Paper No. 2019-001, Cornell Legal Studies Research Paper No.19-44, Oxford Legal

In addition, banks that are owned by holding companies are subject to consolidated supervision of the entirety of the organization and entitled to draw on the parent as a source of strength, factors that are critical for ensuring the safety and soundness of the organization and of the financial system more broadly. Tech payments companies, on the other hand, are not subject to consolidated supervision at the parent company level. "Without a consolidated, holding company supervisor—that is, an agency able to see the big picture and empowered to oversee all subsidiaries, including the unregulated ones—no one outside of the firm can understand how the group operates and how much risk it is taking."[25] Consolidated supervision allows regulators to intervene with troubled institutions before risks accumulate within the organization, thereby mitigating the impact on consumers and the financial system.

The fallout from Wirecard AG's failure illustrates the very real risks that presented by a tech company operating a payments platform without a consolidated supervisor.[26] The European payment processor, which was not subject to consolidated supervision in any jurisdiction, collapsed in 2020, causing substantial harm both to the financial system and to consumers. Hundreds of thousands of small businesses and consumers were left without access to their funds or the ability to process payments for days. Other negative effects cascaded across the financial system, as financial institutions around the world had to write off multimillion-dollar losses because of exposures to the failed company.[27] Had this payments processor been subject to consolidated supervision, the fraud and risk management failures that led to its demise likely could have been detected, avoiding, or at least reducing, the harm suffered by consumers, businesses, and other financial institutions.[28]

Finally, banks are required to implement robust anti-money laundering and anti-terrorist financing programs and are subject to strict sanctions imposed by the Office of Foreign Assets Control. Federal law requires all money services businesses to register with the U.S. Secretary of the Treasury, bringing them within the purview of the Financial Crimes Enforcement Network (FinCEN). To the extent that tech companies engage in activities in which banks engage that present the same or similar BSA/AML or sanctions risks, the CFPB should coordinate with the banking agencies, Treasury, and

---

Studies Research Paper No. 55/2019, Available at SSRN: https://ssrn.com/abstract=3462351 or http://dx.doi.org/10.2139/ssrn.3462351.

25 Hsu at 9.

26 Wirecard AG claimed to process upwards of $140 billion worth of transactions per year on behalf of its customers. Yet, on June 18, it was revealed that nearly $2 billion that the company claimed to be holding in a pair of banks in the Philippines was missing, or perhaps never existed in the first place. The missing funds would have accounted for the corporation's entire profit over the last decade. Wirecard quickly crumbled. Its market cap, which was once nearly $30 billion, now hovers around $75 million. DAX. (2020, October 10). Wirecard AG. Bloomberg. Retrieved from: https://www.bloomberg.com/quote/WDI:GR

27 For example, Commerzbank alone wrote off €175 million in loans made to Wirecard, a greater loss from the scandal than from all COVID-19-related economic fallout, along with multiple other banks and institutions writing off multimillion-dollar losses for the second quarter. Storbeck, O. (2020, August 5). Commerzbank takes greater loan loss from Wirecard than Covid-19 debt. Retrieved from: https://www.ft.com/content/68afa079-90ea-4dba-bf31-85958232d356.

28 *See, e.g.,* Wilmarth, Arthur E. Jr., "Wirecard and Greensill Scandals Confirm Dangers of Mixing Banking and Commerce," 40 Banking & Financial Services Policy Report No. 5 (May 2021), available at: Wirecard and Greensill Scandals Confirm Dangers of Mixing Banking and Commerce (gwu.edu), ("Regulators failed to take timely enforcement actions against Wirecard . . . because they did not exercise consolidated supervisory authority over the complex international" structure created by the firm.).

FinCEN to ensure that these tech companies are subject to the same expectations to combat financial crime.

## IV. Competition and Consumer and Small Merchant Choice Should be Protected.

The scale of large platforms may pressure merchants and other payment providers to participate, while the scale of the platform simultaneously can severely stifle competition and innovation.[29] This introduces risk that large tech payments systems operators "limit consumer choice and stifle innovation by anticompetitively excluding certain businesses."[30]

In circumstances where an ecosystem restricts competitor app developers' access to functionality (e.g., the Near Field Communications chip on a mobile device which enables forms of contactless payments), consumers have less choice in mobile payments options than they otherwise may have.[31] Many platform providers may "self-preference" financial services products on devices by automatically defaulting to their own products (unless manually overridden by the user) and by presenting their own products as "top-of-wallet" over competitor alternatives that may be better suited for the consumer. A company might collect or associate user browsing, device activity or search terms that, when paired with payments data, could allow the platform to design products targeted to the user based on its knowledge of consumer behavior from this data.[32] Using this data could give these companies a further competitive advantage by making it difficult for new companies to enter the market

---

29 *See* BIS Annual Economic Report at 67 ("Big techs' role in financial services brings efficiency gains and lowers barriers to the provision of financial services, but the very features that bring benefits also have the potential to generate new risks and costs associated with market power. Once a captive ecosystem is established, potential competitors have little scope to build rival platforms. Dominant platforms can consolidate their position by raising entry barriers. They can exploit their market power and network externalities to increase user switching costs or exclude potential competitors. Indeed, over time big techs have positioned their platforms as "bottlenecks" for a host of services. Platforms now often serve as essential selling infrastructures for financial service providers, while at the same time big techs compete with these providers. Big techs could favour their own products and try to obtain higher margins by making financial institutions' access to prospective clients via their platforms more costly. Other anticompetitive practices could include "product bundling" and cross-subsidising activities. Given their business model, these practices could reach a larger scale for big techs.") (Internal citations omitted).

30 *See* CFPB Press Release, "CFPB Orders Tech Giants to Turn Over Information on their Payment System Plans" (October 21, 2021), available at: CFPB Orders Tech Giants to Turn Over Information on their Payment System Plans | Consumer Financial Protection Bureau (consumerfinance.gov).

31 For example, the European Commission in June 2020 opened a formal antitrust investigation to assess whether Apple's conduct in connection with Apple Pay violates EU competition rules. The investigation concerns Apple's terms, conditions and other measures for integrating Apple Pay in merchant apps and websites on iPhones and iPads, Apple's limitation of access to the Near Field Communication (NFC) functionality ("tap and go") on iPhones for payments in stores, and alleged refusals of access to Apple Pay. *See* Antitrust: Commission opens investigation into Apple practic (europa.eu).

32 *See* BIS Annual Economic Report at 62 (Tech companies "with a dominant presence in e-commerce collect data from vendors, such as sales and profits, combining financial and consumer habit information. Big techs with a focus on social media have data on individuals and their preferences, as well as their network of connections. Big techs with search engines . . . typically have a broad base of users and can infer their preferences from their online searches. The type of synergies varies with the nature of the data collected. Data from e-commerce platforms can be a valuable input into credit scoring models, especially for SME and consumer loans. Big techs with a large user base in social media or internet search can use the information on users' preferences to market, distribute and price third-party financial services (e.g. insurance) . . . Combining their advanced technology with richer data and a stronger customer focus, big techs have been adept at developing and marketing new products and services.").

or to thrive, as other companies are less likely to have this data to gain insights into consumer behaviors and therefore less likely to be able to develop products specifically targeted to consumer.

Some tech companies have grown their market share by "partnering" with banks that are not subject to the Dodd-Frank Act interchange limits, creating price advantages for those companies that may, at the same time, disadvantage small merchants and consumers. More broadly, as described previously, these tech companies are not subject to the same level of direct, consistent oversight as banks, exposing consumers and the financial system to risks. Customers of these arrangements may not be protected from harm to the same extent they would be if they obtained products or services from institutions operating under comparable standards that apply to entities operating squarely within the federal bank regulatory perimeter. Acting Comptroller Hsu has recognized these risks, noting that these partnerships may "be [characterized as] 'rent-a-charter' arrangements, ***which allow fintechs to skirt a host of rules at the expense of customer protection and bank safety and soundness***," and that the OCC has "concerns about regulatory arbitrage being facilitated by certain [banking-as-a-service] or rent-a-charter arrangements . . . [and has] begun to increase [its] focus on the banks that provide services to large fintechs and facilitate synthetic banking outside of the bank regulatory perimeter. This dovetails with the CFPB's recently announced order requesting data from tech companies to assess the adequacy of their consumer protections."[33] We encourage the CFPB to support the work of the OCC and other regulators in considering whether these arrangements are consistent with consumer protection and safety and soundness laws and objectives.

## V. **Conclusion**.

Innovation in the financial services marketplace has produced and will continue to produce benefits for consumers and the financial system. This innovation in payments and other products and services should be fostered and encouraged. Furthermore, technical innovations may result in new ways of protecting consumers and the financial system, using approaches that are not possible without them. There is a crucial difference, however, between innovation in products, services, and delivery, on the one hand, and innovation in avoiding consumer protection and safety and soundness regulation, on the other hand. The Bureau should ensure that consumers are protected from harm regardless of whether they obtain payments services from a bank or from a company operating outside of the federal bank regulatory perimeter, such as tech companies. In addition, the Bureau should coordinate with the banking regulators and other policymakers to establish a framework to ensure that these companies operate in a safe and sound manner. Innovation should not come at the expense of consumer wellbeing or the safety and soundness of the financial system.

[33] Hsu at 7-8, 13 (emphasis added).

*****

If you have any questions, please contact the undersigned by phone at 703-887-5229 or by email at pparidon@bpi.com.

Sincerely,

Paige P. Paridon

Paige Pidano Paridon
Senior Vice President,
Associate General Counsel
*Bank Policy Institute*

cc: Mark E. Van Der Weide, General Counsel
Michael S. Gibson, Director, Division of Supervision and Regulation
(Board of Governors of the Federal Reserve System)

Nick Podsiadly, General Counsel
Doreen R. Eberley, Director, Division of Risk Management Supervision
(Federal Deposit Insurance Corporation)

Michael J. Hsu, Acting Comptroller of the Currency
Benjamin W. McDonough, Senior Deputy Comptroller and Chief Counsel
(Office of the Comptroller of the Currency)