BANK POLICY INSTITUTE

July 5, 2022

Via Electronic Mail

Diane Farrell
Deputy Under Secretary for International Trade
International Trade Administration
Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 20230

Re: “Developing a Framework on Competitiveness of Digital Asset Technologies” (Docket No. 220509–0112; RIN 0625–XC047)

Ladies and Gentlemen:

The Bank Policy Institute[1] appreciates the opportunity to comment on the Department of Commerce’s Request for Comment on “Developing a Framework on Competitiveness of Digital Asset Technologies” in connection with Executive Order 14067, “Ensuring Responsible Development of Digital Assets.”[2] According to the Fact Sheet accompanying the Executive Order, digital assets, including cryptocurrencies, exceeded a $3 trillion market cap last November, although published reports indicate that recent turmoil in those markets has reduced that number by as much as two-thirds. In addition, some surveys indicated that around 16 percent of adult Americans – approximately 40 million people – have invested in, traded, or used cryptocurrencies. In light of the growth of digital assets over the past few years and the risks that are presented by digital assets and related activities that are not yet subject to a comprehensive regulatory framework, BPI supports the goal of the Executive Order to promote a coordinated, “whole of government” approach to fostering responsible innovation and the following specific policy objectives for digital assets articulated in the Executive Order:

(a) protection of consumers, investors, and businesses in the United States;
(b) protection of United States and global financial stability and the mitigation of systemic risk;
(c) mitigation of illicit finance and national security risks posed by misuse of digital assets;

[1] BPI 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] 87 Fed. Reg. 14143 (March 14, 2022).

(d) reinforcement of U.S. leadership in the global financial system and in technological and economic competitiveness, including through the responsible development of payment innovations and digital assets;
(e) promotion of access to safe and affordable financial services; and
(f) support of technological advances that promote responsible development and use of digital assets.

Section 8(b)(iii) of the Executive Order directs the Secretary of Commerce, in consultation with the Secretary of State, the Secretary of the Treasury, and the heads of any other relevant agencies, to establish a framework for enhancing U.S. economic competitiveness in, and leveraging of, digital asset technologies. We appreciate the Commerce Department's solicitation of input and recommendations as it considers the development of this framework for digital assets.[3]

BPI supports innovation, but believes it must be conducted in a manner consistent with the safety and soundness of the financial system, national security, and robust consumer and investor protection. A coordinated, government-wide approach to establishing a comprehensive framework for regulating digital assets and related activities will help to ensure that the United States remains a global leader in innovation while also ensuring that consumers, the financial system, and national security are protected.

I. A coordinated, whole of government approach will foster responsible innovation and protect the U.S. financial system and consumers.

Digital assets have the potential to provide benefits to consumers and businesses and to the financial system. However, uncertainties remain about the potential risks presented by digital assets. For this reason, a careful, data-driven, and whole-of-government approach for evaluating the potential benefits and risks of, and establishing a regulatory framework to address the risks presented by, digital assets, is prudent.[4] A fractured approach to this evaluation is likely to result in the failure to establish an appropriate, comprehensive regulatory framework for digital assets and related activities, ultimately harming customers and potentially undermining United States competitiveness in these markets.

The risks of an uncoordinated approach to the regulation of digital assets and related activities are real, as illustrated with respect to the activity of safeguarding cryptoassets. Banks have a long history of providing, and are well-suited to provide, safeguarding services. However, although the banking regulators last year promised additional clarity on the authority of banks to engage in crypto

[3] Section 8(b)(iii) of the Executive Order directs the Secretary of Commerce, in consultation with the Secretary of State, the Secretary of the Treasury, and the heads of any other relevant agencies, to (within 180 days of the date of the Executive Order) establish a framework for enhancing U.S. economic competitiveness in, and leveraging of, digital asset technologies.

[4] As defined in the Executive Order, "digital assets" refers to "all [central bank digital currencies (CBDCs)], regardless of the technology used, and to other representations of value, financial assets and instruments, or claims that are used to make payments or investments, or to transmit or exchange funds or the equivalent thereof, that are issued or represented in digital form through the use of distributed ledger technology. For example, digital assets include cryptocurrencies, stablecoins, and CBDCs. Regardless of the label used, a digital asset may be, among other things, a security, a commodity, a derivative, or other financial product. Digital assets may be exchanged across digital asset trading platforms, including centralized and decentralized finance platforms, or through peer-to-peer technologies."

custody activities and related risk management expectations, that guidance has yet to be provided. Thus, banks continue to evaluate options to enter this business but have yet to do so at scale. Meanwhile, apparently without consultation with the federal banking regulators or other stakeholders or market participants, in March, the SEC issued Staff Accounting Bulletin No. 121, which would require an entity – presumably including a banking organization[5] – safeguarding a cryptoasset to present a liability (and recognize a corresponding asset) on its balance sheet equal to the fair value of the safeguarded cryptoasset.[6] This treatment of cryptoassets deviates from existing accounting treatment of safeguarded assets held in a custodial capacity, which does not result in assets or liabilities reported on the custodian's balance sheet because the custodian has no property right in the asset and no liability in the event of deterioration of the value of the asset or otherwise in respect of the cryptoasset. Furthermore, if SAB 121 is interpreted to require the inclusion of custodied cryptoassets on a banking organization's balance sheet, the knock-on effects under the prudential regulatory framework would be so significant that banking organizations effectively would be precluded from providing such services to clients.

The SEC staff has indicated that SAB 121 is driven by investor protection concerns related to legal, technological, and regulatory risks arising from custodied assets. BPI supports the need to mitigate these risks in the interest of investor protection. However, we note that these risks are comprehensively addressed by the legal, regulatory and supervisory frameworks applicable to banking organizations.[7] The lack of communication and coordination among the agencies as well as the lack of consultation on this standard has resulted in the SEC perhaps not fully understanding how these risks are handled differently by different market participants and therefore has resulted in banks' having to pause efforts underway to enter this business as they await further clarity from the agencies about the applicability of SAB 121 and the risk management expectations of their supervisors. Indeed, Federal Reserve Chair Powell noted at a Congressional hearing recently that "Custody assets are off balance sheet, have always been . . . The SEC made a different decision as it relates to digital assets for reasons it explained, and now we have to consider those."[8] Investors and customers will be worse off without the participation of regulated banking organizations in this market, as customers and the market would benefit from the entry of highly regulated banks with sophisticated risk managements capabilities into the crypto custody market. Consistent with the goal of promoting responsible innovation via a "whole of government" approach articulated in the Executive Order, the relevant agencies should jointly

---

[5] SAB 121 discusses an entity whose activities include both operating a crypto-asset platform that allows its users to transact in cryptoassets and providing a service where it will safeguard the platform users' cryptoassets, including maintaining the cryptographic key information necessary to access crypto-assets. We understand, however, that SEC Staff has indicated that it interprets SAB 121 as applying to all instances involving the safeguarding of cryptoassets, regardless of whether the entity also operates a trading platform.

[6] SEC Staff Accounting Bulletin No. 121 (March 31, 2022), available at: SEC.gov | Staff Accounting Bulletin No. 121. "Cryptoasset" is very broadly defined in the SAB to include digital assets issued and/or transferred using distributed ledger or blockchain technology using cryptographic techniques.

[7] There is no indication that the SEC staff took into account this fundamental dichotomy between banking and nonbanking organizations. Nor is there any indication that the SEC staff considered the preclusive effect of SAB 121 on banking organizations in relation to nonbanking organizations. Accordingly, it appears unlikely that the SEC gave appropriate consideration to whether banks should be excluded from the accounting treatment in the SAB or the question of the impact on investor protection if it were not feasible, solely because of SAB 121, for banks to provide custody services for cryptoassets.

[8] Jesse Hamilton, "US Fed Evaluating SEC's Position on Digital Assets Custody, Powell Says," CoinDesk (June 22, 2022), available at: US Fed Evaluating SEC's Position on Digital Assets Custody, Powell Says (coindesk.com)

evaluate the comprehensive legal, regulatory and supervisory frameworks applicable to banking organizations that addresses the risks identified by the SEC and determine that banks should be excluded from the accounting treatment in the SAB, thereby enabling them to provide custody services for cryptoassets.[9] Moreover, future regulatory efforts should involve consultation among responsible agencies to identify this type of conflict with the stated goals of the Executive Order.

II. The potential benefits and risks of digital assets and related activities must be carefully weighed by policymakers.

a. A U.S. retail CBDC is unlikely to provide the benefits its proponents cite and would undermine the commercial banking system, and many of the potential benefits of a CBDC can be achieved through alternative means.

BPI has written extensively about the possible risks and benefits that a U.S. retail CBDC would present and has found that a United States retail CBDC is unlikely to provide the benefits its proponents cite, and, furthermore, would undermine the commercial banking system in the United States by severely constricting the availability of credit to the economy in a highly procyclical way, thereby ultimately harming not just banks, particularly the smallest banks, but consumers and financial stability.[10] In addition, most, if not all, of the potential benefits of a CBDC can likely be achieved through alternative, less harmful means.

For example, although proponents of a CBDC often assert that a CBDC could increase the speed and lower the cost of payments, including cross-border payments, whether this could be achieved in practice is a complex question that many central banks and international bodies are just beginning to study. Furthermore, there are other methods underway of improving payments – both domestically and internationally – that could achieve that goal without CBDC.[11] At a minimum, further research is

---

[9] *See* comment letter re: SAB 121 to the Office of the Chief Accountant of the Securities and Exchange Commission, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Federal Reserve Board, and the Department of the Treasury, June 23, 2022, ABA, BPI, and SIFMA, available at: https://bpi.com/bpi-aba-and-sifma-comment-on-staff-accounting-bulletin-no-121/.

[10] *See* the Bank Policy Institute's work on central bank digital currency, available at https://bpi.com/category/digital-assets/central-bank-digital-currency/.

[11] In the United States, there are other innovations underway that are improving and will continue to improve the domestic payments system. For example, The Clearing House runs its real-time payments system, the RTP network, which enables instantaneous settlement and availability. The Clearing House, "First New Core Payments System in the U.S. in More than 40 Years Initiates First Live Payments" (Nov. 14, 2017) (available at: https://www.theclearinghouse.org/payment-systems/articles/2017/11/20171114-rtp-first-new-core-payments-system). In addition, the Federal Reserve itself is developing a real-time payments system, FedNow, that is scheduled to begin operating in 2023. *See* The Federal Reserve FRBServices.org, "About the FedNow[SM] Service" (2022) (available at: https://www.frbservices.org/financial-services/fednow/about.html). In addition, the FSB has highlighted as a key priority the improvement of cross-border payments and established a roadmap achieve this goal. The G20 countries agreed in 2020 to a multiyear roadmap to identify and deploy improvements to cross-border payments. *See* Financial Stability Board, Enhancing Cross-border Payments: Stage 3 Roadmap (October 13, 2020), available at: Enhancing Cross-border Payments: Stage 3 roadmap (fsb.org). Furthermore, EBA CLEARING, SWIFT and The Clearing House have announced that they plan to launch a pilot service for immediate cross-border (IXB) payments by the end of this year. *See* John Adams, "Banks gearing up to test real-time payments across borders," *American Banker*, (May 2, 2022), available at:

required before drawing any conclusions about the potential benefits of a CBDC in enhancing payments' efficiency or lowering costs.

Similarly, proponents often assert that a CBDC could improve financial inclusion. However, we are unaware of any substantiated use case for CBDC that would benefit low- and moderate-income people, and, moreover, private-sector developments are helping to bring previously unbanked or underbanked individuals into the financial system—for example, through the introduction of low-cost "Bank On" bank transaction accounts.[12] Our research has shown that the take-up rate for Bank On accounts is greatest in areas with high concentrations of lower-income and minority households, as indicated by the ZIP codes associated with the accounts, demonstrating that these bank accounts are successfully addressing customer demand for these types of accounts and making banking more inclusive and accessible.[13]

Finally, as noted previously, an intermediated account-based CBDC would inevitably lead to a reduced level of commercial bank deposits, as customers would trade deposits for CBDC. This reduction in bank deposits would lead to more expensive credit intermediation and a reduction in the supply of credit, as a CBDC would be a source of funding for the Federal Reserve, not for banks, in contrast to customer dollar deposits under the current system.[14]

We believe that legislation would be required to authorize the Federal Reserve or the Executive Branch to issue a CBDC, and, before enacting legislation authorizing a CBDC, Congress should balance the uncertain benefits of a CBDC against the serious risks to the financial system that a CBDC could pose, as well as consider the alternative ways in which the purported benefits of a CBDC may be achieved.

---

https://www.americanbanker.com/payments/news/banks-gearing-up-to-test-real-time-payments-across-borders; *See also* "EBA Clearing, SWIFT, and The Clearing House to deliver pilot service for immediate cross-border payments" (April 28, 2022), available at: EBA CLEARING, SWIFT and The Clearing House to deliver pilot service for immediate cross-border payments (prnewswire.com).

[12] For more information about Bank On, see https://joinbankon.org/. Bank On accounts are certified by the Cities for Financial Empowerment Fund, a non-profit organization, and this type of account comes with a minimum balance requirement of only $25 and monthly fees of $5 or less; account opening is free, as is in-market ATM usage, and there are no overdraft charges. *See* Bank On National Account Standards 2021-2022, available at: https://2wvkof1mfraz2etgea1p8kiy-wpengine.netdna-ssl.com/wp-content/uploads/2020/10/Bank-On-National-Account-Standards-2021-2022.pdf. Bank On certified accounts are now offered by over 110 banks and credit unions at more than 39,000 branches nationwide, and over 3.8 million accounts were open and active in 2020 at just 17 institutions that reported data, and growth increased in 2021. *See* Written Testimony Submitted to the U.S. House Committee on Financial Services, House Subcommittee on Consumer Protection and Financial Institutions. Hearing on "Banking the Unbanked: Exploring Private and Public Efforts to Expand Access to the Financial System," (July 21, 2021), Submitted by David Rothstein, Senior Principal, Cities for Financial Empowerment Fund, available at: hhrg-117-ba15-wstate-rothsteind-20210721.pdf (house.gov); Accounts – BankOn (joinbankon.org); *See also* The Bank On National Data Hub: Findings from 2020, available at: bankonreport_2020findings.pdf (stlouisfed.org).

[13] *See* Calem, Paul, *"Bank On" Transaction Accounts: Making Traditional Banking More Inclusive* (April 13, 2021), available at: https://bpi.com/wp-content/uploads/2021/04/Bank-On-Transactions-Accounts-Making-Traditional-Banking-More-Inclusive.pdf.

[14] *See* Greg Baer and Bill Nelson, BPI, "A Costly Misunderstanding About CBDC" (December 17, 2021), available at: A Costly Misunderstanding About CBDC - Bank Policy Institute (bpi.com).

III. Policymakers should carefully consider the potential risks and potential benefits of digital assets and related activities when considering a regulatory framework to govern their use.

Policymakers should evaluate all of the potential risks and potential benefits that digital assets or related activities may present when considering the development of a regulatory framework to govern their use. For example, the President's Working Group on Financial Markets' Stablecoin Report identifies the risks presented by different types of stablecoins that policymakers should address in establishing how different types of stablecoins should be regulated.[15] The report also identified potential benefits that certain types of appropriately regulated stablecoins could present.[16]

IV. Banks need clarity about the risk management expectations for their involvement in providing digital asset products and services.

BPI also has identified the need for the relevant agencies to further clarify the ability of banks to engage in digital assets-related activities and the risk management expectations related to those activities to foster responsible innovation, as referenced previously with respect to providing custody services for cryptoassets.[17] Banks have traditionally been at the forefront of technological innovation, and as more use cases emerge for digital assets, BPI's members are evaluating where and how these innovations can be applied in their own businesses to best serve the needs of customers (or potential customers). Both the public and the financial system would benefit from banks' involvement in digital assets. Banks are subject to comprehensive and robust risk management, supervision and examination processes, are subject to consumer protection laws and regulations, maintain strong capital buffers,

[15] *See* The President's Working Group on Financial Markets (PWG), the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, "Report on Stablecoins," (Nov. 1, 2021), available at: Report on Stablecoins (treasury.gov). BPI has engaged in a similar evaluation of the possible risks and benefits of stablecoins. *See* Greg Baer, BPI, "Making Stablecoins Stable: Is the Cure Worse than the Disease?", Bank Policy Institute, Sept. 27, 2021, available at https://bpi.com/making-stablecoins-stable-is-the-cure-worse-than-the-disease/.

[16] PWG Stablecoin Report at 1 ("If well-designed and appropriately regulated, stablecoins could support faster, more efficient, and more inclusive payments options.").

[17] The OCC, through Interpretive Letter 1179, requires a banking organization to receive supervisory nonobjection regarding risk management systems and controls before conducting crypto-asset custody activities. OCC Interpretive Letter No. 1179, Chief Counsel's Interpretation Clarifying: (1) Authority of a Bank to Engage in Certain Cryptocurrency Activities; and (2) Authority of the OCC to Charter a National Trust Bank (Nov. 18, 2021); *see also* OCC Interpretive Letter No. 1170, Re: Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers (July 22, 2020). The FDIC imposes similar requirements. *See* FDIC, FIL-16-2022, Notification of Engaging in Crypto-Related Activities (April 7, 2022). The federal banking agencies jointly advised in November 2021 that throughout 2022 they would "provide greater clarity on whether certain activities related to crypto-assets conducted by banking organizations are legally permissible, and expectations for safety and soundness, consumer protection, and compliance with existing laws and regulations related to: crypto-asset safekeeping and traditional custody services; ancillary custody services; facilitation of customer purchases and sales of crypto-assets; loans collateralized by crypto-assets; Issuance and distribution of stablecoins; and activities involving the holding of crypto-assets on balance sheet." Joint Statement on Crypto-Asset Policy Sprint Initiative and Next Steps (November 23, 2021), available at: Joint Statement on Crypto-Asset Policy Sprint Initiative and Next Steps (federalreserve.gov). The agencies have not yet provided additional clarity on these topics.

carry deposit insurance, have well-developed anti-money laundering ("AML") programs[18] including robust know-your-customer ("KYC") practices, and have substantial experience with incorporating new technologies into the financial system. Banks have the resources, talent and expertise to implement robust compliance programs, which is especially important with respect to digital assets, which present novel illicit finance risks.

Failure to provide clarity regarding the expectations for banks in engaging in digital assets related activities is hindering the ability of banks to engage in responsible innovation in this space, thereby requiring consumers to look solely to unregulated or lightly regulated non-bank financial service providers and limited-purpose, uninsured banking institutions for digital asset products and services, instead of banks.[19] Fractured regulation ultimately harms consumers and the financial system. Non-banks and limited-purpose banking institutions offering digital asset products and services are generally not subject to comprehensive and robust supervision and examination or consumer protection regimes, may have thin capital requirements and may not have sufficient resources to cover operational and other losses.[20] Further, some non-banks offer digital asset products that bear similarities to bank products—like interest bearing accounts—even though such products lack FDIC insurance.[21]

V. The requirements and expectations regarding digital assets-related activities should not be lower for financial institutions that operate outside the bank regulatory perimeter.

Policymakers should develop an appropriate regulatory framework for nonbank entities engaged in digital assets-related activities to ensure that those products and activities are subject to equivalent requirements and risk management expectations as would be expected of banking entities engaged in the same activities presenting the same risks.

---

[18] For the purposes of this letter, references to AML practices are inclusive of bank compliance with economic sanctions programs administered by the Office of Foreign Assets Control ("OFAC").

[19] Non-bank financial service providers and limited-purpose banking institutions have been early providers of digital asset products and services. Many products and services offered by limited-purpose banking institutions resemble traditional bank products and activities, including custodial services, payment services and activity akin to deposit-taking. States have established regulatory frameworks supporting non-bank financial services providers' offering of these products. For example, the New York State Department of Financial Services ("NYDFS") has been issuing licenses related to virtual currency business activities, known as BitLicenses, since 2015 pursuant to its virtual currency regulations under the New York Financial Services Law. The NYDFS has also granted limited-purpose trust company charters under the New York Banking Law, giving such entities state authority to act as qualified custodians and exchanges for digital assets. Similarly, in 2019, the State of Wyoming created Special Purpose Depository Institution ("SPDI") charters, Wyo. Stat. § 13-12-101, *et seq.*, authorizing the chartering of institutions focused on digital assets.

[20] *See, e.g.*, BPI, *Beware the Kraken* (Oct. 21, 2020), https://bpi.com/beware-the-kraken/; BPI, *Why a Wyoming Charter is No Hail Mary for the Anti-Fractional Banking Team* (Nov. 9, 2020), https://bpi.com/why-a-wyoming-charter-is-no-hail-mary-for-the-anti-fractional-banking-team/.

[21] Consumers may view such products as equally safe as traditional, FDIC-insured bank deposit accounts. One exchange advertises one such account to customers who are "looking for a dollar-based experience that's more like an interest-bearing savings account . . . ." *See* Coinbase, *How to earn crypto rewards*, https://www.coinbase.com/learn/tips-and-tutorials/how-to-earn-crypto-rewards; Gemini, *What is Gemini Earn?*, https://support.gemini.com/hc/en-us/articles/360055836212-What-is-Gemini-Earn-.

As part of this effort, policymakers should ensure that data protection and cybersecurity requirements and expectations are consistently applied to all entities engaging in digital assets-related activities. BPI has long warned of the dangers of the uneven expectations and requirements regarding consumer data protections and cybersecurity controls for banks versus nonbank fintechs.[22] Banks have developed sophisticated systems to protect consumer data and to detect, prevent, and respond to cyber threats. These activities are subject to extensive regulatory oversight to ensure such protections are in place and can include financial penalties or restrictions on activities for failure to comply. In particular, banks are subject to the Gramm-Leach-Bliley Act and its implementing regulations that require maintaining consumer data privacy, extensive guidelines from the Federal Financial Institutions Examination Council (FFIEC) Information Technology handbooks,[23] and the federal banking agencies' third-party risk management guidelines.[24] As noted, banks, contrasted with nonbanks, are subject to regular examination for compliance with these requirements.

In addition, it is important that consumers are protected regardless of whether they obtain digital asset-related products or services from a regulated banking entity or a fintech. However, nonbanks in the digital asset ecosystem are not subject to regular, direct supervision for their compliance with consumer protection requirements, in contrast to federally regulated banks. Indeed, some tech companies "make technical, and questionable, arguments that their products or services fall

---

[22] *See* comment letter re: National Institute of Standards and Technology – Draft Report 8389 Cybersecurity Considerations for Open Banking Technology and Emerging Standards, Bank Policy Institute, SIFMA and American Bankers Association, March 3, 2022, available at https://bpi.com/wp-content/uploads/2022/03/BPI-Comment-Letter-NIST-Open-Banking-Report.pdf. *See also* BPI Statement Before House Task Force on Financial Technology on Consumer Consumers Access to Personal Financial Data, Sept. 21, 2021, available at https://bpi.com/bpi-statement-before-house-task-force-on-financial-technology-on-consumer-consumers-access-to-personal-financial-data/. *See also* comment letter re: Re: Advance Notice of Proposed Rulemaking on Consumer Access to Financial Records (Docket No. CFPB-2020-0034), Bank Policy Institute, Feb. 4, 2021, available at https://bpi.com/wp-content/uploads/2021/02/BPI-Comment-Letter-Responding-to-CFPB-1033-ANPR-2021.02.04.pdf. *See also* comment letter re: Notice and Request for Comment Regarding the CFPB's Inquiry Into Big Tech Payment Platforms, Consumer Financial Protection Bureau, BPI, Nov. 10, 2021, available at BPI-CommentCFPBBigTechInquiry-12-10-21final.forsubmission-CFPB-2021–0017.pdf; *See also* Comment Letter Re: Request for Information and Comment on Digital Assets (RIN 3064–ZA25), Bank Policy Institute and Consumer Bankers Association, July 16, 2021, available at: Microsoft Word - BPI Comment Letter - FDIC RFI on Digital Assets (FINAL - signed.

[23] FFIEC IT handbooks are used in the supervision of financial institutions and cover topics such as information security, management, technology architecture and operations, and retail payment systems.

[24] The federal banking agencies also have issued "Third Party Risk Management Guidelines" that outline the expectations for banks to manage the risks of counterparties with whom they have business relationships. The agencies recently proposed amendments to this guidance and requested comment on the extent to which banking organization may have "business arrangements" and third-party relationships with data aggregators, and therefore should manage these relationships consistent with the third-party risk management guidance." BPI submitted a comment on the proposed amendments to the TPRM Guidance and stated that data aggregators — including both those that engage in unilateral "screen-scraping" and those with which a banking organization may have a contract or other data sharing relationship — can pose meaningful risks to banking organizations and their customers but that the TPRM practices and expectations described in the Proposed Guidance would not be appropriate for either type of activity for several reasons. However, the ultimate expectations of the regulators in this regard remain unclear at this point. *See* BPI's comment letter in response to the "Proposed Interagency Guidance on Third-Party Relationships," available at: Microsoft Word - BPI Comment Letter - Interagency Guidance on Third Party Relationships (Docket ID(7661407.20).docx.

outside the existing regulatory framework."[25] Further, "the enforcement authority for applicable consumer protection requirements on fintech activities is scattered among various federal and state regulators."[26] 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. Indeed, in the context of several cryptoasset companies, the ownership and executive management are murky, which is, of course, directly contrary to the regulatory requirements for insured banks. Banks, in contrast, have significant experience and expertise in implementing consumer protection safeguards. In addition, banks are subject to regular consumer compliance examinations by the federal banking agencies. To protect consumers, all participants in digital asset ecosystem should be subject to the same requirements and oversight for their privacy and security practices.[27]

Finally, banks are required to implement robust anti-money laundering and countering the financing of terrorism programs as well as comprehensive sanctions compliance programs. While federal AML 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 nonbank fintechs engage in the same activity with the same illicit finance risk characteristics as banks, then the relevant regulators should work together to ensure that these tech companies are subject to the same expectations as banks are to combat financial crime.[28]

Thus, policymakers should ensure that the requirements and expectations regarding digital assets-related activities should not be lower for financial institutions that operate outside the bank regulatory perimeter as compared to banking entities engaged in the same activities presenting the same risks.

---

[25] *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).

[26] *Id*.

[27] *See* comment letter re: National Institute of Standards and Technology – Draft Report 8389 Cybersecurity Considerations for Open Banking Technology and Emerging Standards, Bank Policy Institute, SIFMA and American Bankers Association, March 3, 2022, available at https://bpi.com/wp-content/uploads/2022/03/BPI-Comment-Letter-NIST-Open-Banking-Report.pdf. *See also* comment letter re: Notice and Request for Comment Regarding the CFPB's Inquiry Into Big Tech Payment Platforms, Consumer Financial Protection Bureau, BPI, Nov. 10, 2021, available at BPI-CommentCFPBBigTechInquiry-12-10-21final.forsubmission-CFPB-2021–0017.pdf. *See also* letter re: Updated Proposed Guidelines for Evaluating Account and Services Requests, Board of Governors of the Federal Reserve System, BPI, ABA, CBA, TCH, ICBA, and MBCA, April 22, 2022, available at https://bpi.com/wp-content/uploads/2022/04/BPI-Joint-Trades-Comment-Letter-to-Federal-Reserve-re-Fed-Accounts-Supplemental-Proposal-2022.04.21.pdf. *See also* comment letter re: Request for Information and Comment on Digital Assets (RIN 3064–ZA25), Bank Policy Institute and Consumer Bankers Association, July 16, 2021, available at: Microsoft Word - BPI Comment Letter - FDIC RFI on Digital Assets (FINAL - signed).

[28] *See* Letter to Financial Crimes Enforcement Network, from Bank Policy Institute re: Request for Information and Comment Regarding Review of Bank Secrecy Act Regulations and Guidance (Feb. 14, 2022) (pgs. 30-32), *available at* https://bpi.com/wp-content/uploads/2022/02/BPI-Comments-on-FinCEN-Review-of-Bank-Secrecy-Act-Regulations-and-Guidance.pdf.

* * * * *

We appreciate the opportunity to comment on the Department of Commerce's request for comment. If you have any questions, please contact the undersigned by phone at (703) 887-5229 or by email at paige.paridon@bpi.com.

Respectfully submitted,

Paige P. Paridon

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