December 15, 2022

Via electronic mail to fsb@fsb.org

Financial Stability Board
Basel, Switzerland

Re: Comments on proposed frameworks for the international regulation of crypto-asset activities and global stablecoin arrangements

Ladies and Gentlemen:

The Bank Policy Institute ("BPI") and The Clearing House Association L.L.C. ("TCH")[1] appreciate this opportunity to comment on two documents issued by the Financial Stability Board ("FSB"): (i) the consultative document on the regulation, supervision, and oversight of crypto-asset activities and markets ("Crypto-Asset Consultative Document")[2] and (ii) the consultative report on the review of the FSB's high-level recommendations for the regulation, supervision, and oversight of global stablecoin arrangements ("GSC Consultative Report").[3] BPI and TCH commend the FSB for its work on these issues and fully support the FSB's goal of developing uniform international principles applicable to crypto-asset activities and global stablecoin arrangements.[4]

[1] See Appendix A for information about BPI and TCH.

[2] FINANCIAL STABILITY BOARD, REGULATION, SUPERVISION AND OVERSIGHT OF CRYPTO-ASSET ACTIVITIES AND MARKETS: CONSULTATIVE DOCUMENT (Oct. 11, 2022) (link) (hereinafter CRYPTO-ASSET CONSULTATIVE DOCUMENT).

[3] FINANCIAL STABILITY BOARD, REVIEW OF THE FSB HIGH-LEVEL RECOMMENDATIONS OF THE REGULATION, SUPERVISION AND OVERSIGHT OF "GLOBAL STABLECOIN" ARRANGEMENTS: CONSULTATIVE REPORT (Oct. 11, 2022) (link) (hereinafter GSC CONSULTATIVE REPORT).

[4] The FSB defines a crypto asset as "[a] digital asset (issued by the private sector) that depends primarily on cryptography and distributed ledger or similar technology. Crypto-assets include, but are not limited to, a crypto-asset that is classified as a payment instrument in a jurisdiction and a crypto-asset that is classified as a security in a jurisdiction." *See* CRYPTO-ASSET CONSULTATIVE DOCUMENT, *supra* note 2, at 71. In a 2020 consultative document, the FSB defined a digital asset as "[a] digital representation of value which can be used for payment or investment purposes. This does not include digital representations of fiat currencies. FINANCIAL STABILITY BOARD, ADDRESSING THE REGULATORY, SUPERVISORY AND OVERSIGHT CHALLENGES RAISED BY "GLOBAL STABLECOIN" ARRANGEMENTS: CONSULTATIVE REPORT 4 (Apr. 14, 2020) (link). As neither definition includes central bank digital currency ("CBDC"), BPI and TCH assume that CBDC is outside the scope of these consultations and have not included comments related to CBDCs.

BPI and TCH support innovation but believe it must be conducted in a manner consistent with the safety and soundness of the financial system, anti–money-laundering ("AML") and countering-the-financing-of-terrorism ("CFT") standards, and robust consumer and investor protections.[5] Digital assets and related activities have grown rapidly in recent years and have the potential to provide benefits to consumers and businesses and the financial system, but certain types of digital-asset–related activities present risks that require comprehensive management. In many jurisdictions, including the United States, it is more concerning when nonbanks conduct these activities because there is generally a lack of robust, thorough, and clear regulatory and supervisory frameworks applicable to them.[6]

Authorities must distinguish among digital assets, cryptocurrencies, and tokenized assets, as well as the underlying distributed ledger technology ("DLT") and blockchain infrastructure, which may differ in use across functions and activities, when they apply existing (or develop new) regulatory frameworks for them. As the FSB notes, there are no universally accepted definitions of the terms "crypto assets" and "digital assets."[7] We generally understand the term "digital asset" to be an umbrella term that captures different subsets of assets, such as crypto assets (crypto-native tokens such as bitcoin and ethereum), stablecoins, and CBDCs. In general, the volatility and related risks often cited in connection with "digital assets" refer to risks presented by crypto-native tokens and stablecoins.

To the extent digital-asset–related activities are engaged in by nonbanks, there may be other risks presented because those entities are generally not subject to a comprehensive regulatory framework (and, indeed, are often subject only to a very limited regulatory framework, or even none at all, and have very limited corporate governance controls). This contrasts sharply with banks, which are subject to, among other requirements, stringent risk-based capital and liquidity, AML/CFT, risk management, and cybersecurity requirements. Furthermore, banks, unlike nonbanks, are subject to

---

[5] The private sector stands ready to accelerate digital-asset innovation and to increase digital-asset activity within the regulatory perimeter. As one example, the Regulated Liability Network proof of concept to tokenize commercial bank, central bank, and electronic money on the same chain offers the promise of delivering a next-generation digital money format based on national currency units (*e.g.*, denominated in U.S. dollars). *See* Press Release, Members of the U.S. Banking Community Launch Proof of Concept for a Regulated Digital Asset Settlement Platform (Nov. 15, 2022), *available at* businesswire.com (link). As another example, Partior, a shared-ledger multicurrency clearing platform, was launched as a technology company by JPMorgan, DBS, and Temasek in 2021. *See* Press Release, JPMorgan Chase & Co., DBS, J.P. Morgan and Temasek to Establish Platform to Transform Interbank Value Movements in a New Digital Era (Apr. 28, 2021) (link). Partior is designed to perform atomic clearing and settlement on a 24x7 basis among participating institutions using blockchain and smart-contract technology. *See Partior Aims to Become the World's Ledger for Banks*, DIGFIN (May 15, 2022) (link); *The Global Ambitions of Partior, the JP Morgan, DBS Blockchain Payment System*, LEDGER INSIGHTS (Nov. 16, 2022) (link).

[6] We use the term "nonbank" in this response generally to refer to an entity without a banking charter or license, although we note there may be some entities in the United States with banking charters or licenses that do not have federal deposit insurance and the resultant comprehensive regulatory scheme. Institutions like these may warrant additional regulation and oversight if they engage in crypto-related activities, especially if they seek access to central bank accounts and services. See discussion in section III below regarding nonbank and less-regulated entity access to central bank accounts and services in the context of stablecoin issuance.

[7] As the FSB notes in the Crypto-Asset Consultative Document, some jurisdictions apply a "catch-all" definition that includes all digital assets. Others have provided more granular regulatory definitions. Authorities appear to use different terminology, including "digital asset," "crypto asset," "virtual asset," "virtual currency," and "convertible virtual currency." *See* CRYPTO-ASSET CONSULTATIVE DOCUMENT, *supra* note 2, at 9.

supervision and examination for adherence to those requirements. Therefore, our recommendations generally are directed to nonbank entities and other entities not subject to robust regulation, supervision, and examination that engage in crypto-asset–related and stablecoin activities.[8] In some cases, however, our recommendations encompass broader digital-asset–related activities carried on by nonbank entities.

By contrast, we assume that the terms "digital asset" and "crypto asset"—and therefore, our response to the consultations—exclude tokenized versions of traditional assets issued by banks subject to consolidated supervision, such as tokenized bank deposits and tokenized securities. This is because the comprehensive regulatory framework, supervision, and examination to which banks are subject addresses potential risks arising from those assets and from banks' related activities. Our comments also do not address risks associated with a CBDC.[9] Likewise, our comments relating to stablecoins are directed at nonbank stablecoin issuers and special-purpose, uninsured depository institutions not subject to consolidated supervision.

The FSB's consultations would benefit from additional clarity that traditional banking products and activities utilizing DLT, blockchain, or other novel technologies are excluded from the scope of the consultations for two key reasons. First, banks appropriately manage risks that may be presented by using any particular technology to perform standard recordkeeping functions internal to a bank. BPI's and TCH's member banks use technology only if they determine the associated risks could be appropriately managed consistent with their risk appetites and risk management capabilities. Second, banking organizations, at least in most major jurisdictions, are subject to a comprehensive regulatory framework and consolidated supervision and therefore do not present the same risks as unregulated or less-regulated entities engaged in crypto activities. In many jurisdictions, such frameworks, including those that help ensure strong customer identification/identity verification, AML/CFT screening, and sanctions compliance processes, are in place. In the United States, that is certainly the case with respect to insured, federally supervised banks. Banks are also subject to extensive and comprehensive regulation, supervision, and examination for compliance with prudential, consumer protection, and data privacy requirements, among others. Larger banking organizations have special, separate examinations of, among other areas, custody and technology. This supervisory oversight includes the robust evaluation of information technology ("IT") risk management, internal controls, and cybersecurity risk management. Banking organizations also must meet regulatory expectations with respect to other operational resiliency obligations and recovery and resolution planning mandates.[10] Adherence to these

[8] For example, in the United States, our recommendations would generally apply to certain state-chartered, uninsured depository institutions that are not subject to federal supervision and regulation that are formed for a limited purpose, such as issuing stablecoins or facilitating other crypto-related activities.

[9] With respect to a potential retail U.S. CBDC, TCH and BPI have previously explained why they believe the risks outweigh any potential benefits and should lead to the conclusion that a CBDC should not be adopted. *See* Letter from Robert C. Hunter, TCH, to Ann E. Misback, Secretary, Board of Governors of the Federal Reserve System, 3–10 (May 20, 2022) (link); Letter from Paige Pidano Paridon, BPI, to Ann E. Misback, Secretary, Board of Governors of the Federal Reserve System (May 20, 2022) (link).

[10] Banking organizations are subject to exams that evaluate how well management addresses risks related to the availability of critical financial products and services, including risks arising from cyber events. Management must also ensure the adoption of processes to oversee and implement resiliency, continuity, and response capabilities

standards is monitored by the oversight and review of dedicated teams of on- and offsite examiners from federal banking agencies.

This comprehensive regulatory risk management framework distinguishes banking organizations from nonbanks, protects clients (including consumers), and promotes safety and soundness regardless of the activities in which banking organizations are engaged. For example, with respect to providing custodial services, banks are required to segregate their custody function from other functions and are prohibited from using client funds for their own purposes. Banks are then subject to direct, consistent supervision and examination to ensure they abide by those requirements. Furthermore, as financial institutions subject to comprehensive prudential regulation and supervision, BPI's and TCH's member banks would engage in digital-asset–related activities only if they determined the associated risks could be appropriately managed consistent with their risk appetites and risk management capabilities and consistent with supervisory expectations.

We believe it is imperative that authorities consider the effectiveness of banking entities' controls and of oversight for their compliance with relevant requirements if they propose to engage in activities using novel technologies. The Monetary Authority of Singapore ("MAS") did so when it proposed no "additional reserve backing and prudential requirements on banks that issue [single-currency–pegged stablecoins] by tokenising liabilities of the bank, given that banks are already subject to stringent risk-based capital and liquidity, ML/TF, technology risk management and other requirements under the Banking Act."[11]

Banks have the resources, talent, and expertise to implement robust compliance programs to manage the risks presented by certain products and services involving digital and crypto assets. For this reason, both the public and the financial system would benefit from banks' involvement in these markets, as banks could provide products and services within the regulatory perimeter in which they operate. The FSB should highlight this distinction between regulated banks and nonbanks and, as described further below, encourage local authorities to clarify the authority of banks to engage in digital-asset–related activities and related risk management expectations to the extent the authorities have not clearly defined these concepts. The standards that apply to nonbanks should be no less rigorous than those that would apply to regulated banking entities if they were to engage in the same activities, as less rigorous standards would lead to arbitrage and consumer and investor harm. The risk of regulatory arbitrage is not merely real but is being realized and is increasing.

I. Overview

Section I of this letter identifies risks that crypto assets and related activities conducted by nonbanks and other unregulated entities pose to the financial system, investors, consumers, and businesses. These risks warrant attention and coordination and must be promptly addressed, both within and across jurisdictions. We also highlight some of our recommendations related to the Crypto-Asset Consultative Document, which are described in more detail in section II.

---

to safeguard employees, customers, and products and services. *See* Federal Financial Institutions Examination Council, FFIEC INFORMATION TECHNOLOGY EXAMINATION HANDBOOK: BUSINESS CONTINUITY MANAGEMENT (Nov. 2019) (link).

[11] *See* MONETARY AUTHORITY OF SINGAPORE, PROPOSED REGULATORY APPROACH FOR STABLECOIN-RELATED ACTIVITIES: CONSULTATION PAPER 8 (Oct. 26, 2022) (link).

The market capitalization of all cryptocurrencies increased sharply in recent years, from about $300 billion in June 2018 to close to $3 trillion by late 2021.[12] Since then, market capitalization has decreased sharply, such that it now appears to be under $900 billion.[13] Some surveys have indicated that around 16 percent of American adults—approximately 40 million people—have invested in, traded, or used cryptocurrencies; the latter figure is no doubt significantly larger globally.[14]

Yet this growth and extraordinary volatility have occurred in an ecosystem without comprehensive and consistent supervision and examination of cryptocurrency or stablecoin issuers and arrangements, as well as one that bars the most highly regulated financial institutions from participating. Matters routinely addressed in the supervision and examination processes of regulated financial institutions—such as capital and liquidity, reserve maintenance and management, operational risk, third-party risk management, data security, data privacy, and AML/CFT and sanctions compliance—often go unaddressed, exposing the market and end users to the resulting risks on an ongoing basis.[15] The Crypto-Asset Consultative Document calls particular attention to these issues in Annex 1, which lists crypto activities, the types of entities that provide them, associated vulnerabilities and risks, and potentially relevant international standards and policies.[16] Highly regulated entities such as banks are already subject to the types of standards and policies cited in the annex. Other types of entities often are not, which means those risks and vulnerabilities will likely be left unaddressed.

These risks are not merely theoretical. For example, some nonbank stablecoin arrangements have completely collapsed;[17] issuers have decided to abruptly shut down operations or have failed, and

---

[12] *See* CoinMarketCap, Total Cryptocurrrency Market Cap, Global Cryptocurrency Charts (link) (estimating the total market capitalization of the cryptocurrency market at $2.9 trillion as of November 9, 2021); TODD PHILLIPS & ALEXANDRA THORNTON, CENTER FOR AMERICAN PROGRESS, CONGRESS MUST NOT PROVIDE STATUTORY CARVEOUTS FOR CRYPTO ASSETS (Mar. 1, 2022) (noting the collective crypto asset market capitalization peak of $2.9 trillion in November 2021) (link); Michael J. Hsu, Acting Comptroller of the Currency, Remarks Before the Institute of International Economic Law at Georgetown University Law Center: Thoughts on the Architecture of Stablecoins 2 (Apr. 8, 2022) (estimating the overall size of the cryptocurrency market at "around $2 trillion" and suggesting a decline from a peak earlier in 2022) (link).

[13] *See* CoinMarketCap, *supra* note 12, (estimating the total market capitalization of the cryptocurrency market at $858.8 billion as of December 9, 2022). *See also* CoinGecko, Cryptocurrency Prices by Market Cap (link) (reporting aggregate cryptocurrency market capitalization of $893 billion as of December 10, 2022).

[14] The White House, Fact Sheet, White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets (Sept. 16, 2022) (link).

[15] Although some proponents of stablecoins suggest that state money transmitter licensing regimes are sufficient to address the risks presented by stablecoins, state money transmitter licensing regimes largely predate the development of stablecoins, are often not fit (at least not fully fit for purpose), are not uniform, and may not even cover stablecoin arrangements at all. Refer to footnote 26 for a more detailed explanation of why they fall short.

[16] *See* CRYPTO-ASSET CONSULTATIVE DOCUMENT, *supra* note 2, at 26–39.

[17] *See* Alexander Osipovich & Caitlin Ostroff, *TerraUSD Crash Led to Vanished Savings, Shattered Dreams*, WALL STREET JOURNAL (May 27, 2022); *The Next Stablecoin Collapse Could Be a Lot Worse*, WASHINGTON POST (June 2, 2022).

crypto-asset service providers have frozen accounts and cut off customers' access to their assets;[18] arrangements have suffered massive, sudden shocks due to internal and external manipulation and attack, including cyberattack;[19] issuers have been found to have made material misrepresentations about the assets "backing" their coins;[20] arrangements have suffered from developmental difficulties and design challenges;[21] and misuse has presented significant concerns about money laundering and terrorist financing.[22]

Most recently, turmoil was set off in the cryptoverse when FTX Trading Ltd. ("FTX"), one of the largest digital currency exchanges, filed for bankruptcy and billions of dollars of customer assets were found to be missing.[23] FTX is alleged to have misused client funds and, according to its new chief executive officer, to have lacked sufficient "controls and basic corporate standards such as 'accounting, audit, cash management, cybersecurity, human resources, risk management, data protection and other systems.'"[24] On December 13, a series of criminal and civil charges were brought against the founder of FTX, Samuel Bankman-Fried.[25]

---

[18] *See, e.g.,* Macro Quiroz-Gutierrez, *Customers of Bankrupt Crypto Lending Service Voyager Digital Are Offered a Way to Access Some of Their Frozen Funds*, FORTUNE (July 22, 2022); Maria Ponnezhath & Tom Wilson, *Major Crypto Lender Celsius Files for Bankruptcy*, REUTERS (July 14, 2022); Vicky Ge Huang, *Big Crypto Lender Celsius Freezes All Account Withdrawals*, WALL STREET JOURNAL (June 13, 2022).

[19] *See, e.g.*, Olga Kharif et al., *Hackers Steal $100 Million by Exploiting Crypto's Weak Link*, BLOOMBERG (June 24, 2022); Cheyenne Ligon, *North Korean Hacking Group Behind $100M Horizon Bridge Hack: Report*, COINDESK (updated June 30, 2022); Jonathan Ponciano, *Second Biggest Crypto Hack Ever: $600 Million in Ether Stolen From NFT Gaming Blockchain*, FORBES (Mar. 29, 2022); Emily Nicolle, *Crypto.com Suspends Withdrawals After 'Unauthorized Activity*,' LOS ANGELES TIMES (Jan. 17, 2022) (noting that cryptocurrency and stablecoin wallet provider crypto.com stopped all deposits and withdrawals while investigating "unauthorized activity" and that Coinbase, Binance, and Kraken all experienced outages in 2021).

[20] *See* In the Matter of Investigation by Letitia James, Attorney General of the State of New York, of iFINEX Inc. et al. Settlement Agreement (Feb. 18, 2021), 3–13 (link) (finding that material misrepresentations had been made about the backing of Tether). *See also* Zeke Faux, *Anyone Seen Tether's Billions?* BLOOMBERG (Oct. 7, 2021) (examining Tether's backing, as well key officers of Tether).

[21] *See* Nivesh Rustgi, *Algorithmic Stablecoin Crashes 50% as Devs Scramble for a Fix* CRYPTO BRIEFING (Apr. 7, 2021) (noting that the algorithmic stablecoin FEI suffered price instability due to a protocol mishap, forcing holders to choose between a reduced value holding (a "lower peg value") and accepting a penalty of 50 percent for exchanging their FEI). *See also* Ryan Clements, *Built to Fail: The Inherent Fragility of Algorithmic Stablecoins*, 11 WAKE FOREST L. REV. ONLINE 131 (Oct. 25, 2021) (noting that algorithmic stablecoins have design flaws that make them inherently unstable).

[22] Indeed, the U.S. Treasury Department proposed an action plan to address such risks. *See* U.S. DEPARTMENT OF THE TREASURY, ACTION PLAN TO ADDRESS ILLICIT FINANCING RISKS OF DIGITAL ASSETS 4 (Sept. 16, 2022) (link).

[23] *See* David Yaffe-Bellany, *Embattled Crypto Exchange FTX Files for Bankruptcy*, NEW YORK TIMES (Nov. 11, 2022).

[24] Rohan Goswami, *Never Seen 'Such a Complete Failure' of Corporate Controls, Says New FTX CEO Who Also Oversaw Enron Bankruptcy*, CNBC (Nov. 17, 2022) (link) (quoting incoming CEO John Ray III).

[25] *See* Press Release, U.S. Attorney's Office, Southern District of New York, United States Attorney Announces Charges Against FTX Founder Samuel Bankman-Fried: Bankman-Fried Charged in an Eight-Count Indictment with Fraud, Money Laundering, and Campaign Finance Offenses (Dec. 13, 2022) (link); Press Release, U.S. Securities and Exchange Commission, SEC Charges Samuel Bankman-Fried with Defrauding Investors in Crypto Asset Trading

Banks, on the other hand, are required to implement robust governance and risk management structures. They must separate safekeeping operations from trading and other similar activities when they hold client assets in custody. Banks are obligated to segregate each client's assets, not just from the bank's proprietary assets, but also from all other clients' assets. Banks are also prohibited from rehypothecating or using the financial assets of their custody customers.

Fundamentally, consumers, investors, and businesses must have a clear understanding of the benefits and risks of digital assets, as well as an understanding of how digital assets differ from traditional products, so they can make informed decisions. Many nonbank entities engaged in crypto activities do not provide adequate or accurate disclosures about the activities they conduct or the risks presented by their businesses, however. In the United States, while some nonbank entities engaged in crypto-related activities may be subject to state money transmitter licensing schemes, those are insufficient to address these issues and risks and are not a substitute for federal prudential regulation, supervision, and examination.[26]

Instead, new laws, or revisions to existing laws, are necessary to ensure appropriate disclosure by nonbank entities, including, but not limited to, disclosures about their operations, risk profiles, financial condition, conflicts of interest, the products they provide and activities they conduct, the regulatory oversight to which they are subject, transactions with affiliates, and any government safety net to which they may have resort. In addition to these disclosures, nonbank entities should be subject to auditing by independent certified public accountants with appropriate expertise. (Insured banks are already subject to requirements for independent audits.) Nonbank entities should also be required to institute appropriate consumer protections and transaction risk allocations and to operate with business models that enable them to absorb potential losses.

Platform FTX: Defendant Concealed His Diversion of FTX Customers' Funds to Crypto Trading Firm Alameda Research While Raising More Than $1.8 Billion from Investors (Dec. 13, 2022) (link); Press Release, U.S. Commodity Futures Trading Commission, CFTC Charges Sam Bankman-Fried, FTX Trading and Alameda with Fraud and Material Misrepresentations (Dec. 13, 2022) (link).

[26] Although some states have addressed the inadequacy of state money transmitter licensing schemes as they relate to cryptocurrency and stablecoins by enacting regulations specifically targeting digital currencies, the vast majority of states have yet to do so, leaving the potential for significant coverage gaps across the United States. Even if state money transmitter laws do apply to cryptocurrency and stablecoins, they are likely inadequate in numerous ways. For example, state money transmitter laws do not provide for supervision of entities at the holding company level, which is important given that the cryptocurrency/stablecoin arrangements that could scale the fastest would likely be associated with an already existing fintech platform. Additionally, many state money transmitter laws and the regulations promulgated under them do not impose third-party and vendor risk management requirements, and some state money transmitter laws fail to impose portfolio restrictions or restrictions on the use of customer funds or transactions with affiliated entities or individuals, and may not contain adequate capital or liquidity requirements, important factors given that the value of stablecoins must be backed by highly liquid assets in order to protect consumer investments. *See* Letter from Robert C. Hunter, TCH, to Chairman Sherrod Brown & Ranking Member Patrick J. Toomey, Senate Banking Committee (Feb. 11, 2022) (link) (providing a statement for the record on stablecoins and stablecoin arrangements and discussing state money transmitter licensing schemes). *See also* Michael J. Hsu, Acting Comptroller of the Currency, Remarks to the Harvard Law School and Program on International Financial Systems Roundtable on Institutional Investors and Crypto Assets, Don't Chase 4 (Oct. 11, 2022) (link) (noting that money transmission regulation is quite different from bank regulation).

BPI and TCH have consistently asserted that the appropriate response to the risks to consumers, investors, and businesses presented by the growth of stablecoins issued by nonbanks and the risks presented by other cryptocurrencies is regulation and support the recommendations made in the report on stablecoins issued by the President's Working Group on Financial Markets ("PWG"), the Federal Deposit Insurance Corporation ("FDIC"), and the Office of the Comptroller of the Currency ("OCC").[27]

In some jurisdictions, authorities have taken initial, targeted steps to address certain risks crypto assets and crypto-asset ecosystems pose. In the European Union, for example, provisional agreement on the markets in crypto assets (MiCA) proposal lays the groundwork for certain protections for consumers and, among other things, would require crypto-asset service providers to obtain an authorization from a national authority prior to operating, require offerors of or entities seeking to trade crypto assets to disclose certain material information about the assets, including the rights and obligations attached to the crypto assets, the underlying technology used for such assets, and related risks, and require stablecoin issuers to hold capital.[28]

As a further example, the MAS has proposed protections for crypto-asset users as part of a Payment Services Act that would require "digital payment token service providers," including crypto-asset issuers, to provide disclosures on design, risks, and redemption rights, hold reserve assets in cash, cash equivalents, or short-dated sovereign debt securities at 100 percent or more of the par value of digital assets, and comply with prudential requirements, including capital requirements.[29] As noted, the MAS proposal would not impose "additional reserve backing and prudential requirements on banks that issue [single-currency-pegged stablecoins] by tokenising liabilities of the bank" in light of the robust prudential oversight and regulation to which banks are already subject.[30]

In other jurisdictions like the United States, however, authorities have generally taken only limited enforcement actions, rather than developing comprehensive regulatory schemes, to address specific nonbanks engaged in crypto activities that have harmed consumers and investors. For example, the Securities and Exchange Commission ("SEC") fined the crypto exchange BlockFi $100 million for its crypto lending product that offered variable monthly returns because the SEC determined that it was an unregistered security.[31] This enforcement action also prompted the SEC to issue an investor bulletin on crypto-asset interest-bearing accounts, warning investors that interest-bearing accounts for crypto-asset

---

[27] *See* PRESIDENT'S WORKING GROUP ON FINANCIAL MARKETS, FEDERAL DEPOSIT INSURANCE CORPORATION, & OFFICE OF THE COMPTROLLER OF THE CURRENCY, REPORT ON STABLECOINS (Nov. 2021) (link).

[28] *See Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (MiCA*) (Oct. 5, 2022) (link). *See also* Press Release, Council of the European Union, Digital Finance: Agreement Reached on European Crypto-Assets Regulation (MiCA) (June 30, 2022) (link).

[29] *See* Press Release, Monetary Authority of Singapore, MAS Proposes Measures to Reduce Risks to Consumers from Cryptocurrency Trading and Enhance Standards of Stablecoin-Related Activities (Oct. 26, 2022) (link).

[30] MONETARY AUTHORITY OF SINGAPORE, *supra* note 11, at 8.

[31] Press Release, U.S. Securities and Exchange Commission, BlockFi Agrees to Pay $100 Million in Penalties and Pursue Registration of its Crypto Lending Product (Feb. 14, 2022) (link). The SEC also found that BlockFi made a false and misleading statement for more than two years on its website concerning the level of risk in its loan portfolio and lending activity. *Id.*

holdings "may sound similar to interest-bearing accounts with a bank or credit union, but investors need to be aware that these crypto asset-related accounts are not as safe as bank or credit union deposits."[32] BlockFi has since filed for bankruptcy as a result of its exposure to FTX.[33]

Voyager, another crypto-lending platform, suspended all trading, deposits, withdrawals, and rewards and filed for bankruptcy in July 2022.[34] Voyager is alleged to have misled its customers into thinking the money they had invested with Voyager was insured by the FDIC and was therefore much safer than it was. The Board of Governors of the Federal Reserve System ("Federal Reserve Board") and the FDIC issued a joint letter demanding that Voyager cease and desist from making false and misleading statements regarding its FDIC deposit insurance status.[35] The same day, the FDIC issued an advisory reminding insured banks "they need to be aware of how FDIC insurance operates and need to assess, manage, and control risks arising from all third-party relationships, including those with crypto companies."[36]

While agencies' use of their existing authorities to address specific risks presented by certain crypto activities carried out by nonbank entities in targeted, after-the-fact actions is an important initial step to address these risks, broader regulatory and supervisory frameworks must be established to comprehensively address the risks of crypto activities to consumers, investors, and the financial system before the risks spill over and cause such harm.

For these reasons, we believe that global principles to guide home-country development of comprehensive frameworks applying standards and oversight to address the risks presented by crypto assets are essential to preserving financial stability and protecting consumers, investors, and businesses worldwide. We further believe that consistency among frameworks both within and across jurisdictions is critical and note the importance, as these principles and frameworks are developed, of ensuring that banks are no less able to engage in digital-asset–related activities as nonbanks are and of ensuring that banks are not subjected to additional requirements or penalties for conducting traditional banking activities with new technology. As noted previously, banks should not, for instance, be subjected to additional capital requirements for issuing tokenized deposits as they are already subject to a robust, comprehensive capital framework.[37] Nor should they be subject to additional requirements, including capital requirements, if they provide custody services for digital assets or use DLT, blockchain, or other newer technologies for internal recordkeeping purposes.

---

[32] *See* U.S. Securities and Exchange Commission, Investor Bulletin: Crypto Asset Interest-Bearing Accounts (Feb. 14, 2022) (link).

[33] *See* Alexander Gladstone, *Crypto Lender BlockFi Follows FTX Into Bankruptcy*, WALL STREET JOURNAL , Nov. 28, 2022.

[34] *See* Quiroz-Gutierrez, *supra* note 18.

[35] *See* Letter from Seth P. Rosebrock, Assistant General Counsel, Federal Deposit Insurance Corporation & Jason A. Gonzalez, Assistant General Counsel, Board of Governors of the Federal Reserve System, to Stephen Ehrlich, Chief Executive Officer, & David Brosgol, General Counsel, Voyager Digital, LLC (July 28, 2022) (link).

[36] Federal Deposit Insurance Corporation, Advisory to FDIC-Insured Institutions Regarding FDIC Deposit Insurance and Dealings with Crypto Companies 2 (July 29, 2022) (link).

[37] The MAS has proposed to take this approach, as noted previously. *See* MONETARY AUTHORITY OF SINGAPORE, *supra* note 11.

As a prime example, there are existing regulations and requirements for the design, operation, and maintenance of banks' internal books and records. All books and records systems of a bank, and any new replacement systems, are already subject to supervisory frameworks applying standards and oversight to address risks associated with these systems. Changing the technical design philosophy of a bank's internal books and records from a more traditional database design to a blockchain or DLT-based design does not change the underlying activity and should be evaluated based on the existing supervisory framework. Though at first blush one might be tempted to misclassify or misconstrue internal books and records that rely on a blockchain design as "tokens," simply because the nature of the technology used, the electronic book entries present in such a recordkeeping system serve the identical functional purpose as electronic book entries that are used to record assets in traditional electronic books and records systems. These digital book entries cannot leave the bank's internal books and records as they merely represent records of a bank's accounts. Accordingly, the use by a bank of blockchain or DLT for internal recordkeeping purposes and accompanying internal electronic book entries should not be subject to any additional regulation beyond the existing supervisory framework applicable to a bank's internal books and records systems. Nor should they be subject to any additional capital requirements. Additional regulation or capital charges targeting a specific technology without regard to the underlying activity may impede the ability of well-regulated and -supervised banking institutions to responsibly innovate and adopt new technology.

II. Feedback on the FSB's Proposed Recommendations on Crypto-Asset Activities and Markets

BPI and TCH provide the following comments on the proposed recommendations in the Crypto-Asset Consultative Document.

1. Authorities should have the appropriate powers and tools, and adequate resources, to regulate, supervise, and oversee crypto-asset activities and markets, including crypto-asset issuers and service providers, as appropriate.

BPI and TCH agree with this recommendation.

As noted in section I, crypto assets present numerous risks. As we have recommended previously,[38] the only way to mitigate these risks is to adopt a comprehensive regulatory and supervisory framework at the national level that addresses each risk posed by crypto-asset companies, their subsidiaries, affiliates, and other related entities active in that ecosystem. The standards that apply to these crypto-asset firms should be no less rigorous than those that would apply to regulated banking entities if they were to engage in the same activities, as less rigorous standards would lead to arbitrage and consumer and investor harm.

[38] *See* Letter from Philip Keitel, TCH, to U.S. Department of the Treasury (Nov. 3, 2022) (link); Letter from Philip Keitel, TCH, to U.S. Department of the Treasury (Aug. 8, 2022) (link); Letter from Paige Paridon Pidano, BPI, to Daniel J. Harty, Director, Office of Capital Markets, U.S. Department of the Treasury (Aug. 8, 2022) (link); Letter from Gregg Rozansky, BPI, to Jon Fishman, Assistant Director, Office of Strategic Policy, Terrorist Financing, and Financial Crimes, U.S. Department of the Treasury (Nov. 3, 2022) (link).

Furthermore, given the borderless nature of crypto assets, it is critical that frameworks are consistent across borders. Certain jurisdictions may be further along in developing comprehensive frameworks to address the risks presented by crypto assets, activities, and nonbank firms than others.[39] In the United States, there are gaps in existing regulatory schemes that could allow risks to develop or increase that could harm consumers, investors, businesses, and financial stability. The Financial Stability Oversight Council ("FSOC") has identified three such gaps in the regulation of crypto-asset activities in the United States (and there may be others):

1. The spot markets for crypto assets that are not securities are subject to limited direct federal regulation. As a result, those markets may not feature robust rules and regulations designed to ensure orderly and transparent trading, prevent conflicts of interest and market manipulation, and protect investors and the economy more broadly.

2. Crypto-asset businesses do not have a consistent or comprehensive regulatory framework and can engage in regulatory arbitrage. Some crypto-asset businesses may have affiliates or subsidiaries operating under different regulatory frameworks, so no single regulator may have visibility into the risks across the entire business.

3. Several crypto-asset trading platforms have proposed offering retail customers direct access to markets by vertically integrating the services provided by intermediaries such as broker-dealers or futures commission merchants. Financial stability and investor protection implications may arise from retail investors' exposure to certain practices commonly proposed by vertically integrated trading platforms, such as automated liquidation.[40]

In response to these gaps, the FSOC recommended that:

1. Congress pass legislation to give rulemaking authority to federal financial regulators for crypto assets that are not securities trading in spot markets;
2. Measures be undertaken to address regulatory arbitrage, including coordination among regulators, the enactment of federal legislation to create a comprehensive prudential framework for stablecoin issuers that addresses the financial stability risks posed by stablecoins, the enactment of legislation to give regulators the authority to have supervise the activities crypto asset entity affiliates and subsidiaries, and the use of existing authorities and the enactment of new authorities to ensure crypto asset service providers rare adequately overseen; and

[39] The European Union and Singapore are two examples, as discussed above.

[40] FINANCIAL STABILITY OVERSIGHT COUNCIL, REPORT ON DIGITAL ASSET FINANCIAL STABILITY RISKS AND REGULATION 5, 112–18 (2022) (link). Such vertical integration is sometimes characterized as nonintermediated arrangements, whereby customers can directly access markets. But, as the FSOC's report cautions, "[f]inancial stability implications may arise from vertically integrated platforms' approaches to managing risk from the leverage or credit they offer." *Id.* at 118. Vertically integrated platforms may liquidate under-margined positions without making margin calls, sometimes as frequently as multiple times a minute, which can create "cascading liquidations and reduced capacity for human intervention during periods of stress…." *Id.* Direct exposure of retail investors to these rapid liquidations likewise presents investor and consumer protection issues. *Id*.

3. FSOC member agencies conduct a study of potential vertical integration by crypto-asset firms.[41]

With respect to the third recommendation, the case of FTX may prove instructive, as the entity's failure to segregate activities and risks or to establish appropriate governance or controls is alleged to have contributed to its collapse.[42]

Given the rapidly changing digital-asset ecosystem and lack of clarity about how existing regulatory regimes apply to emerging digital-asset products and services, authorities should continue to "review existing regulations and take steps to clarify regulatory requirements applicable to crypto-asset products and services, address novel fraudulent practices, and enhance disclosure requirements," as suggested by the U.S. Treasury Department.[43]

Home-country authorities should also take stock of the existing powers they have with respect to digital assets, including stablecoins, and identify gaps that need to be filled via legislative, regulatory, or other action and take steps to address those gaps. This assessment should include gaps that arise from the application of existing regulatory and supervisory frameworks to digital assets, as is illustrated by the FSOC example provided above, as well as other gaps that may become apparent as frameworks for crypto and other digital assets are developed. Monitoring for gaps is thus an important part of the ongoing oversight of digital assets—and the entities involved in those assets—that authorities must undertake.

2. Authorities should apply effective regulation, supervision, and oversight to crypto-asset activities and markets—including crypto-asset issuers and service providers—proportionate to the financial stability risk they pose, or potentially pose, in line with the principle "same activity, same risk, same regulation."

BPI and TCH support this recommendation and endorse the principle of "same activity, same risk, same regulation."

This principle promotes consistent application of important legal protections and requirements, mitigates the risk of regulatory arbitrage, and helps avoid customer confusion. The FSOC highlighted several guiding principles that member agencies should consider in evaluating the applicability of existing authorities over the crypto-asset ecosystem, the first of which is "same activity, same risk, same regulatory outcome."[44]

In that vein, requirements and expectations regarding digital asset-related activities should not be lower for entities that operate outside the current regulatory perimeter than they are for regulated

---

[41] *Id.* at 111.

[42] *See* Goswami, *supra* note 24.

[43] U.S. DEPARTMENT OF THE TREASURY, CRYPTO-ASSETS: IMPLICATIONS FOR CONSUMERS, INVESTORS, AND BUSINESSES 51 (Sept. 2022) (link).

[44] *See* REPORT ON DIGITAL ASSET FINANCIAL STABILITY RISKS AND REGULATION, *supra* note 40, at 111.

financial institutions.[45] Rather, domestic policymakers should develop appropriate regulatory frameworks for nonbank entities engaged in digital or crypto-asset-related activities to ensure that those activities are subject to the same stringent requirements and risk management expectations that banking entities engaged in the same activities face. In many jurisdictions, including the United States, banks maintain strong capital and liquidity buffers and are subject to robust, comprehensive risk management, supervision, and examination processes to ensure their safety and soundness. In addition, they are subject to consumer protection laws and regulations and to direct oversight for compliance with those requirements, carry deposit insurance, have well-developed AML/CFT programs,[46] including robust know-your-customer ("KYC") practices, and have substantial experience with incorporating new technologies into the financial system. To the extent that nonbanks present risks that those requirements are intended to address, they should be subject to requirements and oversight that are no less stringent.

In some jurisdictions, including the United States, regulated banks need clarity about risk management expectations for digital-asset products and services**.** BPI and TCH have previously identified the need for the relevant U.S. agencies to further clarify the ability of banks to engage in digital-asset–related activities and the risk management expectations related to those activities so responsible innovation can be fostered.[47]

A regulatory framework should not stifle responsible innovation by banks. At the same time, nonbanks that provide the same or similar services in the digital space should be regulated in accordance with their size and complexity and the risks presented by their activities, consistent with the "same activity, same risk, same regulation" principle articulated in the recommendation. A lack of clarity regarding the expectations and boundaries from the U.S. banking regulators for banks that

---

[45] *See* Letter from Paige Pidano Paridon, BPI, to Diane Farrell, Deputy Under Secretary for International Trade, International Trade Administration, Department of Commerce 7–9 (July 5, 2022) (link).

[46] For the purposes of this letter, references to AML practices are generally meant to be inclusive of compliance with economic sanctions programs, though we occasionally refer explicitly to sanctions compliance for particular emphasis.

[47] The OCC requires banking organizations to receive supervisory nonobjection regarding risk management systems and controls before conducting crypto-asset custody activities. *See* Office of the Comptroller of the Currency, *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*, Interpretive Letter No. 1179 3–4 (Nov. 18, 2021) (link); *see also* Office of the Comptroller of the Currency, *Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers*, Interpretive Letter No. 1170 (July 22, 2020) (link). The FDIC imposes prior-notice requirements for engaging in digital-asset–related activities. *See* Federal Deposit Insurance Corporation, *Notification and Supervisory Feedback Procedures for FDIC-Supervised Institutions Engaging in Crypto-Related Activities*, FIL 16-2022 (Apr. 7, 2022) (link). As does the Federal Reserve. *See* Board of Governors of the Federal Reserve System, *Engagement in Crypto-Asset-Related Activities by Federal Reserve-Supervised Banking Organization*s, SR 22-6 / CA 22-6 (Aug. 16, 2022) (link). The federal banking agencies jointly advised in November 2021 that they would provide greater clarity in 2022 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" relating to a variety of topics involving crypto assets and stablecoins. Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, & Office of the Comptroller of the Currency, Joint Statement on Crypto-Asset Policy Sprint Initiative and Next Steps (Nov. 23, 2021) (link). The agencies have not yet provided additional clarity on these topics.

engage in certain traditional activities using DLT is hindering the ability of banks to engage in responsible innovation in this space—innovation that could potentially strengthen the resilience of the financial system.

For example, banks have come to recognize that DLT is a secure method of recordkeeping that may have the potential to drive efficiencies and reduce systemic risk. As a result of the current regulatory uncertainty banks face, consumers are often limited to engaging solely with unregulated or lightly regulated nonbank financial service providers and limited-purpose, uninsured banking institutions for digital asset products and services instead of federally insured banks.[48] Fractured regulation ultimately harms consumers and the financial system. Nonbanks 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 or no capital requirements, and may not have sufficient resources to cover operational and other losses even when their activities carry the same level of risk, or even higher risk, than the activities conducted by banks and other traditional financial institutions.[49] Some nonbanks offer digital asset products that bear similarities to bank products—like interest-bearing accounts—even though such products lack FDIC insurance.

It is critical that consumers are protected regardless of whether they obtain digital-asset–related products or services from a regulated entity, such as a bank, or from a fintech company or other unregulated entity. Yet nonbanks active in the digital asset ecosystem—unlike federally supervised banks—may not be subject to regular, direct supervision for compliance with consumer protection requirements. The diffuse organizational structure of many tech companies and their lack of clear governance structures raise questions about who is responsible for consumer compliance and about the mechanisms they have to ensure that consumer protections are respected and that they operate in a safe and sound manner. Indeed, the ownership and executive management of several crypto-asset companies are murky, which sharply contrasts with how insured banks operate. Banks have significant experience and expertise in implementing consumer-protection safeguards. In addition, most banks are subject to regular consumer compliance examinations by the Consumer Financial Protection Bureau ("CFPB") or one of the federal banking agencies.

---

[48] Nonbank financial service providers and limited-purpose banking institutions have been early providers of digital-asset products and services. Many products and services that are offered by limited-purpose banking institutions resemble traditional bank products and activities, including custodial services, payment services, and activity akin to deposit-taking. Some states have also established regulatory frameworks supporting nonbank 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. *See* 23 NEW YORK CODES, RULES, AND REGULATIONS § 200.3. The NYDFS has also granted limited-purpose trust company charters under the New York Banking Law (*see* NEW YORK BANKING LAW § 102-a), giving such entities authority to act as qualified custodians and exchanges for digital assets. *See also* Press Release, New York Department of Financial Services, NYDFS Grants Charter to "Gemini" Bitcoin Exchange Founded by Cameron and Tyler Winklevoss: Three Virtual Currency Firms Have Now Received Charters or Licenses from NYDFS—Gemini, Circle, itBit (Oct. 5, 2015) (link). Similarly, in 2019, the state of Wyoming created a special-purpose depository institution charter for institutions focused on digital assets. *See* WYO. STAT. § 13-12-101–126 (2021).

[49] *See, e.g.*, BPI, *Beware the Kraken* (Oct. 21, 2020) (link); BPI, *Why a Wyoming Charter Is No Hail Mary for the Anti-Fractional Banking Team* (Nov. 9, 2020) (link).

Furthermore, policymakers should ensure that data protection and cybersecurity requirements and expectations are consistently applied to all entities engaging in digital-asset–related activities. BPI and TCH have long warned of the dangers of uneven requirements and expectations regarding consumer data protections and cybersecurity controls for banks versus nonbank fintechs.[50] Banks and other regulated entities have developed sophisticated systems to protect consumer data and to detect, prevent, and respond to cyber threats. Banks and other regulated entities are generally subject to extensive regulatory oversight to ensure such protections are in place; financial penalties or restrictions on activities can result if they fail to comply with these obligations.

For example, banks in the United States are subject to the Gramm–Leach–Bliley Act and its implementing regulations, which obligate banks to safeguard their customers' information, extensive IT guidance from the Federal Financial Institutions Examination Council ("FFIEC"),[51] and guidance from the federal banking agencies on third-party risk management.[52] As noted, banks, unlike nonbanks, are subject to regular examination and supervision. All entities engaging in the crypto-related ecosystem should be required to abide by these same requirements and be subject to the same level of examination and supervision.

It is critical that participants in digital-asset transactions be subject to AML/CFT requirements consistent with those that apply to participants in transactions with the same or similar illicit finance risks.[53] In most major jurisdictions, banks are required to implement robust AML and CFT programs, as well as comprehensive sanctions compliance programs. To the extent that nonbanks or uninsured banks not subject to federal supervision at the depository institution and holding company levels (where

---

[50] *See* Letter from Paige Pidano Paridon, BPI, Melissa MacGregor, Securities Industry and Financial Markets Association, & Rob Morgan, American Bankers Association, to National Institute of Standards and Technology (Mar. 3, 2022) (link); Letter from Robert C. Hunter, TCH, to National Institute of Standards and Technology (Mar. 3, 2022) (link). *See also* Letter from Paige Paridon Pidano, BPI, to Consumer Financial Protection Bureau (Dec. 10, 2021) (link); BPI, BPI Statement Before House Task Force on Financial Technology on Consumer Consumers Access to Personal Financial Data" (Sept. 21, 2021) (link); Letter from Dafina Stewart, BPI, & André B. Cotton, Consumer Bankers Association, to James P. Sheesley, Assistant Executive Secretary, Federal Deposit Insurance Corporation (July 16, 2021) (link)' Letter from Naeha Prakash, BPI, to Consumer Financial Protection Bureau (Feb. 4, 2021) (link).

[51] 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.

[52] The federal banking agencies have issued third-party risk management guidelines that outline the expectations for banks to manage the risks of parties with whom they have business relationships. The agencies proposed amendments to this guidance last year. *See* Proposed Interagency Guidance on Third-Party Relationships: Risk Management, 86 Federal Register 38182 (proposed July 19, 2021) (link).

[53] We note that new technologies may emerge in this space that could support compliance with AML/CFT/KYC requirements. For example, BPI has previously expressed support for proposed legislation that would establish a federal task force to identify a digital ID implementation strategy across federal, state, and local governments in a way that is user friendly and accessible and that enhances security and preserves privacy. *See* Press Release, BPI, BPI Supports Senate Effort to Achieve Digital ID Benefits (Sept. 28, 2022) (link). *See also* Letter from BPI et al. to Speaker Pelosi, Republican Leader McCarthy, Majority Leader Schumer, & Republican Leader McConnell (Nov. 18, 2022) (link) (supporting passage of the Improving Digital identity Act of 2022).

relevant) engage in the same activity as banks, they should be subject to the same requirements and expectations as banks to combat financial crime.[54]

Governments should recognize and take actions to mitigate illicit finance risks associated with digital-asset transactions, which may include reduced transparency, disintermediation of financial institutions subject to AML and CFT obligations, increased complexity, and other risks. For example, in the U.S. context, BPI and TCH have each submitted comments on the U.S. Treasury Department's proposed action plan to address illicit financing risks of digital assets.[55] The associations believe that the Treasury Department, working with other relevant offices and agencies of the U.S. government, should ensure the following principles and steps are considered in developing regulations and taking other actions designed to mitigate the illicit finance risks that digital assets and digital-asset transactions pose:

1. The requirements and expectations in respect of AML and CFT activities should be consistent for all institutions that engage in equivalent activities with similar illicit finance risk characteristics, regardless of a particular entity's status as a bank, money services business, or other type of institution.
2. The Treasury Department should recognize and take actions to mitigate the illicit finance risks associated with specific digital assets and digital-asset transactions, such as risks relating to reduced transparency and visibility for law enforcement, disintermediation of financial institutions subject to the Bank Secrecy Act ("BSA"), and increased complexity.
3. U.S. authorities should continue their efforts to implement the Anti-Money Laundering Act of 2020 ("AML Act").[56] These efforts, including facilitation of the AML Act's statutory purposes of reinforcing the risk-based nature of financial institution AML programs and encouraging technological innovation in AML compliance, will be important to mitigate illicit finance risks posed by digital assets and digital-asset transactions.
4. The Treasury Department should facilitate cross-border cooperation and other information sharing relating to the illicit finance risks of digital assets and digital-asset transactions.

Similar steps should be taken in other jurisdictions to mitigate illicit finance risks and ensure a consistent approach to addressing such risks around the world.[57]

With respect to crypto-asset–related networks or payment systems that are or are likely to become systemically important, BPI and TCH support full application of the Principles for Financial

---

[54] *See* Letter from Angelena Bradfield, BPI, to Policy Division, Financial Crimes Enforcement Network (Feb. 14, 2022) (link) (urging action in to address illicit finance risks, including those arising in connection with cryptocurrencies and other emerging payment methods); Letter from Robert C. Hunter, TCH, to Policy Division, Financial Crimes Enforcement Network (Feb. 14, 2022) (link) (focusing on risks posed by nonbank stablecoin arrangements).

[55] *See* ACTION PLAN TO ADDRESS ILLICIT FINANCING RISKS OF DIGITAL ASSETS, *supra* note 22. For BPI and TCH comments on the action plan, refer to footnote 38.

[56] *See* Pub. L. No. 116–283, §§ 6001–6112, 134 Stat. 3388, 4547–64 (2021).

[57] *See* Appendix B for a description of specific illicit finance risks presented by certain digital-asset technologies and in the digital-asset ecosystem more generally and of ways governments can address those risks.

Market Infrastructures ("PFMI") to the operators of such networks or systems to help protect financial markets from the risks they pose.[58] We note that application of the PFMI may not be suitable for innovation involving decentralized systems or public blockchain. So as not to impede regulated entities from innovating using these technologies, we recommend that the FSB and local authorities study how the PFMI might apply to decentralized systems or assets with a decentralized issuer and whether different or additional considerations would be more appropriate.[59]

3. Authorities should cooperate and coordinate with each other, both domestically and internationally, to foster efficient and effective communication, information sharing and consultation in order to support each other as appropriate in fulfilling their respective mandates and to encourage consistency of regulatory and supervisory outcomes.

BPI and TCH agree with this recommendation and have previously stated that a coordinated, whole-of-government approach would foster responsible innovation and help protect consumers, investors, and the financial system.

The technology underlying digital assets has the potential to provide benefits to consumers and businesses and to the financial system. Nevertheless, because of the potential risks presented by certain activities in the digital-assets space, including stablecoin-related activities, it would be prudent to have a coordinated, comprehensive, government-wide approach in local jurisdictions to evaluate the potential benefits and risks of digital assets and to establish a regulatory framework to address the risks they pose. As previously noted, "crypto-assets and related intermediaries are subject to unique and evolving operational risks, including cyber risks. As such, active collaboration and coordination is necessary to ensure that crypto-asset products and services are subject to, and in compliance with, appropriate supervision, oversight, regulation, collection, and disclosure requirements."[60]

A fractured approach to evaluating the risks of various digital-asset categories is likely to result in the failure to establish an appropriate, comprehensive regulatory framework for digital assets and related activities, including stablecoin activities, which could ultimately harm customers and, potentially, the financial system. The risks of an uncoordinated approach to the regulation of digital assets and related activities include regulatory arbitrage, which could allow risks to build up outside the view of any

---

[58] *See* COMMITTEE ON PAYMENT AND SETTLEMENT SYSTEMS AND TECHNICAL COMMITTEE OF THE INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS, PRINCIPLES FOR FINANCIAL MARKET INFRASTRUCTURES (Apr. 2012) (link).

[59] We note that the Committee on Payments and Market Infrastructures and the Board of the International Organization of Securities Commissions previously highlighted this issue in the context of a consultation on the application of the PFMI to stablecoin arrangements. *See* COMMITTEE ON PAYMENTS AND MARKET INFRASTRUCTURES & BOARD OF THE INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS, APPLICATION OF THE PRINCIPLES FOR FINANCIAL MARKET INFRASTRUCTURES TO STABLECOIN ARRANGEMENTS: CONSULTATIVE REPORT (Oct. 2021) (link). In its response to that consultation, TCH made this same recommendation, stating "The decentralized nature of [distributed networks] requires as well further consideration on the application of the principles, in particular the one related to governance." Letter from Robert C. Hunter, TCH, to Committee on Payments and Market Infrastructures & Board of the International Organization of Securities Commissions 5 (Dec. 1, 2021) (link).

[60] U.S. DEPARTMENT OF THE TREASURY, CRYPTO-ASSETS: IMPLICATIONS FOR CONSUMERS, INVESTORS, AND BUSINESSES, *supra* note 43, at 52.

governmental authority and thereby threaten financial stability and result in consumer and investor harm.

As highlighted previously, as part of this coordinated approach, regulators should first create clear definitions of various types of digital assets that capture the different risks they pose and seek to develop a common understanding, both within jurisdictions and across borders, of the meaning of other relevant terms in the crypto-asset ecosystem. Today, digital assets, though they may carry varying levels of risk, are often nevertheless broadly categorized, as noted previously. The term "stablecoin," for instance, is applied to a broad category of assets with varying levels of risk depending on factors such as whether the coin in question is algorithmic or "backed" by assets.[61] Defining important terms and developing a comprehensive lexicon for the various types of digital and crypto assets and entities active within the digital-asset ecosystem will help authorities more effectively target the unique risks that each present.

In addition, information sharing and coordination among agencies are critical to addressing risks, including illicit finance risks, presented by entities operating in the rapidly changing crypto-asset ecosystem. As the U.S. Treasury Department has noted, "[c]rypto-assets are continually evolving, as is the illegal activity that uses crypto-assets. To ensure broad and consistent enforcement and to supplement private sector analytics tools, regulators and law enforcement officials should, as appropriate, share information regarding the type and scale of fraudulent, misleading, or manipulative market practices they are observing and investigating. For example, sharing data could help identify relevant clusters of unlawful activity and spot trends in scams and fraud types."[62] BPI and TCH also support the Treasury's recommendation that law enforcement and regulators continue to coordinate and combat fraud to deter unlawful behavior and improve practices in crypto-asset markets.[63]

Coordination at the international level is also important given the cross-border nature of crypto-markets, which "creates regulatory, supervisory and enforcement challenges," including "risks of regulatory arbitrage or evasion, in which some actors may be incentivised to structure their businesses to circumvent the application of certain jurisdictions' more stringent regulatory requirements."[64] Sharing information on a cross-border basis would help authorities "mitigate material risks of contagion," including information sharing about enforcement actions taken in one jurisdiction against an entity operating in other jurisdictions.[65]

---

[61] See Appendix C for a description of various types of stablecoins.

[62] U.S. DEPARTMENT OF THE TREASURY, CRYPTO-ASSETS: IMPLICATIONS FOR CONSUMERS, INVESTORS, AND BUSINESSES, *supra* note 43, at 51.

[63] *See* Letter from Philip Keitel to U.S. Department of the Treasury, *supra* note 38; Letter from Gregg Rozansky to Jon Fishman, *supra* note 38.

[64] CRYPTO-ASSET CONSULTATIVE DOCUMENT, *supra* note 2, at 12.

[65] *Id.* at 20.

4. **Authorities, as appropriate, should require that crypto-asset issuers and service providers have in place and disclose a comprehensive governance framework. The governance framework should be proportionate to their risk, size, complexity and systemic importance, and to the financial stability risk that may be posed by the activity or market in which the crypto-asset issuers and service providers are participating. It should provide for clear and direct lines of responsibility and accountability for the functions and activities they are conducting.**

BPI and TCH support this recommendation.

One of the risks presented by entities operating in the crypto-asset ecosystem is the lack of robust governance structures. Often, there is little clarity regarding ownership, management responsibilities, or other aspects related to the governance of those entities. That can make it difficult for customers or authorities to understand who is in charge and may lead to challenges in holding the appropriate actors accountable for the entities' actions or compliance with whatever regulatory requirements might apply. Furthermore, as the FSB has noted, "A lack of strong governance . . . could create or exacerbate financial stability concerns."[66]

Governance arrangements may not properly align incentives of decisionmakers and users, which can lead to breakdowns in governance or appropriate decision-making.[67] Indeed, the FSOC has reported that governance breakdowns have arisen frequently in the crypto-asset ecosystem, "sometimes leading to the complete collapse of crypto-asset firms," and has cited several examples of such breakdowns.[68] In addition to human-related governance issues, certain crypto entities use automated management processes, which do not allow for human intervention, even where it might be appropriate or necessary.[69]

Therefore, authorities should require entities in the crypto-asset ecosystem to adopt comprehensive governance frameworks with direct lines of responsibility and accountability, all of which should be subject to disclosure and consistent oversight for maintaining such a governance structure, consistent with how banks operate and are overseen today.

5. **Authorities, as appropriate, should require crypto-asset service providers to have an effective risk management framework that comprehensively addresses all material risks associated with their activities. The framework should be proportionate to their risk, size, complexity, and systemic importance, and to the financial stability risk that may be posed by the activity or market in which they are participating. Authorities should, to the extent necessary to achieve regulatory outcomes comparable to those in traditional finance, require crypto-asset issuers to address the financial stability risk that may be posed by the activity or market in which they are participating.**

---

[66] *Id.* at 12.

[67] *See* FINANCIAL STABILITY OVERSIGHT COUNCIL, *supra* note 40, at 72–73.

[68] *Id.* at 73.

[69] *Id.* at 72.

BPI and TCH support this recommendation.

As noted, certain crypto assets and related activities and nonbank entities operating in the digital asset ecosystem present numerous risks to users, as well as illicit finance and national security risks[70] and systemic and global financial stability risks.

The requirements and expectations regarding entities operating in the crypto ecosystem outside the bank regulatory perimeter should not be lower than those that apply to banks engaged in the same activities.[71] Policymakers should develop an appropriate regulatory framework for nonbank entities engaged in digital-asset–related activities to ensure that those activities are subject to requirements and risk management expectations that are no less stringent than those that would be expected of banking entities engaged in the same activities presenting the same risks. Such a framework should account for risk management and mitigation methods applied to similar activities conducted within the regulatory perimeter, such as capital, liquidity, risk management, cybersecurity, consumer protection, and AML/CFT standards.

For example, the recommendation appropriately notes the importance of supervising and regulating custodial wallet service providers to address the adequate safeguarding of customer assets (e.g., through segregation requirements for client assets, including in the case of the default or bankruptcy of the custodial wallet service provider, and the separation of banking and commercial activities), as well as the maintenance of adequate capital and liquidity. These practices are consistent with the fundamental principles governing custodial activities by regulated financial institutions, including with respect to digital assets: functional separation of safekeeping operations from trading and other similar activities; the segregation of client assets from proprietary assets; and the maintenance of proper control over client assets, which, in the digital space, requires control of the private keys so as to eliminate any single point of failure in the record of ownership. These same requirements should be applied to nonbank entities that provide custodial services.

The FSB should make clear that authorities should adopt third-party risk management requirements and expectations for nonbank crypto-asset service providers consistent with those that apply to banks, particularly in light of the extensive interconnections and relationships that exist among entities operating within the crypto-asset ecosystem that could increase further in light of the recent collapses of numerous firms active in the space and potential acquisitions by rival nonbank firms and exchanges engaged in crypto-related activities.[72] For example, to the extent nonbank entities outsource

[70] The growth and reach of cryptocurrency/stablecoins, the degree to which they permit anonymity, their usability, exchangeability for fiat currency, and other characteristics all present AML/CFT risks that must be addressed as part of the development of a comprehensive prudential framework that applies standards to digital assets that are equivalent to those that apply to insured banks engaged in functionally similar activities.

[71] *See* Letter from Paige Pidano Paridon to Diane Farrell, *supra* note 45, at 7–9.

[72] *See* FINANCIAL STABILITY OVERSIGHT Council, *supra* note 40, at 34–40.

[72] *See* Jack Schickler & Cheyenne Ligon, *FTX, Binance Deal Draws Antitrust Concern*, COINDESK (Nov. 8, 2022); Hannah Lang & Tom Wilson, *Binance Plans to Buy Rival FTX in Bailout as Crypto Market Crumbles*, REUTERS (Nov. 8, 2022) (noting that the proposed sale of the non-U.S. business of FTX, a top-five crypto exchange, to Binance, the world's largest, raised antitrust concerns). Of course, these plans were announced before FTX filed for bankruptcy.

core recordkeeping functions, they should be subject to the same level of risk management requirements to which banks are subject when they outsource core processes to third parties. In the United States, banks are subject to the federal banking agencies' third-party risk management guidance, which outlines the expectation that banking organizations adopt risk management practices that are commensurate with the level of risk and complexity of their respective third-party relationships.[73] Nonbanks should be held to the same standard.

As noted, banks are subject to comprehensive and robust risk management expectations, supervision, and examination processes. To the extent that nonbanks engaging in crypto activities present risks that those requirements and expectations are intended to address, nonbanks should be subject to equivalent requirements, expectations, and oversight.

6. **Authorities, as appropriate, should require that crypto-asset issuers and service providers have in place robust frameworks for collecting, storing, safeguarding, and the timely and accurate reporting of data, including relevant policies, procedures and infrastructures needed, in each case proportionate to their risk, size, complexity and systemic importance. Authorities should have access to the data as necessary and appropriate to fulfil their regulatory, supervisory and oversight mandates.**

BPI and TCH support this recommendation.

As noted previously, policymakers should ensure that data protection and cybersecurity requirements and expectations are consistently applied to all entities engaging in crypto-asset–related activities and should generally ensure that such entities are not subject to less stringent standards than those that apply to entities within the regulatory perimeter that engage in functionally similar activities. BPI and TCH have long warned of the dangers of uneven expectations and requirements regarding consumer data protections and cybersecurity controls for banks versus nonbank fintechs. Banks and other regulated entities have developed sophisticated systems to protect consumer data and to detect, prevent, and respond to cyber threats. Banks and other regulated entities are generally subject to extensive regulatory oversight to ensure such protections are in place; they may face financial penalties or restrictions on their activities if they fail to comply with their obligations.

Reportedly, Binance is now considering bidding for the assets of bankrupt lending platform Voyager Digital. *See* Ian Allison, *Binance to Relaunch Bid for Bankrupt Crypto Lender Voyager: Source*, CoinDesk (Nov. 17, 2022).

[73] As noted above (see footnote 52), the federal banking agencies have each issued third-party risk management guidelines that outline the expectations for banks to manage the risks of parties with whom they have business relationships. The agencies proposed joint amendments to this guidance in 2021 to "offer a framework based on sound risk management principles for banking organizations to consider in developing risk management practices for all stages in the life cycle of third-party relationships that takes into account the level of risk, complexity, and size of the banking organization and the nature of the third-party relationship." Proposed Interagency Guidance on Third-Party Relationships: Risk Management, 86 Federal Register 38182, 38182 (proposed July 19, 2021) (link). BPI and TCH each submitted comments on this proposal. *See* Letter from Gregg L. Rozansky, BPI, to Ann E. Misback, Secretary, Board of Governors of the Federal Reserve System, Chief Counsel's Office, Office of the Comptroller of the Currency, & James P. Sheesley, Assistant Executive Secretary, Federal Deposit Insurance Corporation (Oct. 18, 2021) (link); Letter from Robert C. Hunter, TCH, to Ann E. Misback, Secretary, Board of Governors of the Federal Reserve System, Chief Counsel's Office, Office of the Comptroller of the Currency, & James P. Sheesley, Assistant Executive Secretary, Federal Deposit Insurance Corporation (Oct. 18, 2021) (link).

U.S. banks that provide custodial services for crypto assts and that manage private-key technology are expected to maintain robust data privacy and cybersecurity controls, as well as comprehensive business continuity and resiliency protocols. Nonbanks, by contrast, may be subject to few or no regulatory requirements and may receive no meaningful supervision or partial supervision (e.g., at the entity level but not the holding company level). Authorities should require consistent application of, and oversight for compliance with, requirements related to the collecting, storing, safeguarding, and timely and accurate reporting of data, including record retention.

To monitor potential risks that could arise in the crypto-asset ecosystem, authorities should ensure that they have access to information regarding the activities of crypto-asset issuers and service providers necessary to assess potential risks in a manner similar to supervised banking institutions. In some cases, they may need to implement comprehensive data collection processes for gathering information from crypto-asset issuers and service providers about their activities to do so.[74] International coordination and collaboration, including with respect to data collection and information sharing about potential risks or threats, are also important given the cross-border nature of the crypto ecosystem.

7. Authorities should require that crypto-asset issuers and service providers disclose to users and relevant stakeholders comprehensive, clear, and transparent information regarding their operations, risk profiles and financial conditions, as well as the products they provide and activities they conduct.

BPI and TCH support this recommendation.

Consumers, investors, and businesses must have a clear understanding of the benefits and risks of digital assets, as well as an understanding of how digital assets may differ from traditional assets and payment instruments and rails so they can make informed decisions. In many jurisdictions, new laws, or revisions to existing laws, may be necessary to ensure that comprehensive disclosures are required to enable consumers and investors to understand the risks presented by crypto-asset issuers and service providers and to make informed decisions about whether to engage in activities in the crypto-asset ecosystem.[75] New laws, or revisions to existing laws, may also be needed to address the contracts and contractual provisions underlying crypto assets and crypto-asset services to ensure full and accurate disclosure and fair practices. Clear contracts are the bedrock of traditional financial services, including the provision of custody services. The FSB has cited custody services as an area where disclosure by

[74] *See* Michael J. Hsu, Acting Comptroller of the Currency, Remarks at DC Fintech Week 2022, Skeuomorphism, Commingling, and Data Gaps in Crypto 9 (Oct. 11, 2022) (link).

[75] *See, e.g.,* False Advertising, Misrepresentations of Insured Status, and Misuse of the FDIC's Name or Logo, 87 Federal Register 33415 (June 2, 2022) (FDIC final rule elaborating on what constitutes false advertising of the protections of federal deposit insurance); Press Release, Consumer Financial Protection Bureau, CFPB Takes Action to Protect Depositors from False Claims About FDIC Insurance (May 17, 2022) (link) (announcing release of an enforcement memorandum, noting that misuse of the name or logo of the FDIC, and deceptive representations about deposit insurance, have taken on "renewed importance" in light of crypto-assets, stablecoins, and other emerging financial technologies). *See also* Davis Polk & Wardwell LLP, *A Shot Across the Fintech Bow—The FDIC's Reported Investigation of Voyager Digital* (July 19, 2022) (link); Allyson Versprille, *FDIC Probing How Bankrupt Crypto Broker Voyager Marketed Itself*, BLOOMBERG (July 7, 2022).

nonbank entities in the crypto-asset space may be insufficient. Consumers, investors, and businesses engaging with crypto assets should expect the same level of clarity and transparency from those entities as they can expect from banks.

In the United States, the lack of clear understanding of risks has been highlighted by the U.S. Treasury, which has observed that crypto-asset users "may not be fully aware" of the risks of default or theft of crypto assets "given crypto-asset market participants' frequent emphasis on trading profits with minimal reference to losses, as well as the general lack of comprehensive disclosure."[76] Part of the problem, the FSOC has observed, is that "[m]any nonbank firms in the crypto-asset ecosystem have advertised themselves as regulated. Firms often emphasize money services business regulation, though such regulation is largely focused on anti-money laundering controls or consumer protection requirements and does not provide a comprehensive framework for mitigating financial stability vulnerabilities arising from other activities that may be undertaken, for example, by a trading platform or stablecoin issuer."[77] In addition, the FSOC has found some crypto-asset entities have made false or misleading statements about the availability of federal deposit insurance for their products, which has "given customers the impression that they are protected by the government safety net when they are not. Further, misrepresentations by crypto-asset firms about how they are regulated have also confused consumers and investors regarding whether a given crypto-asset product is regulated to the same extent as other financial products."[78]

Thus, regulators must require and enforce robust, accurate disclosures by entities in the crypto-asset ecosystem. These disclosures should include, but not be limited to, disclosures about their operations, risk profiles, financial condition, conflicts of interest, the products they provide and activities they conduct, the regulatory oversight to which they are subject, transactions with affiliates, and any government safety net to which they may have resort. Robust and accurate disclosures are critical to help crypto-asset users meaningfully consider the risks presented by crypto-asset products and services and make informed decisions as to whether or to what extent to engage in the crypto-asset ecosystem.

8. Authorities should identify and monitor the relevant interconnections, both within the crypto-asset ecosystem, as well as between the crypto-asset ecosystem and the wider financial system. Authorities should address financial stability risks that arise from these interconnections and interdependencies.

BPI and TCH support this recommendation.

In the United States, the FSOC has asserted that crypto-asset activities could pose risks to the stability of the U.S. financial system if their interconnections with the traditional financial system or their overall scale were to grow without being subject to appropriate regulation and supervision.[79] While

[76] U.S. DEPARTMENT OF THE TREASURY, CRYPTO-ASSETS: IMPLICATIONS FOR CONSUMERS, INVESTORS, AND BUSINESSES, *supra* note 43, at 51.

[77] Financial Stability Oversight Council, Fact Sheet, The Financial Stability Oversight Council's Report on Digital Asset Financial Stability Risks and Regulation 2 (Oct. 3, 2022) (link).

[78] *Id.*

[79] *Id.* at 1.

current interconnections with the traditional financial system are relatively limited, these interconnections could potentially increase rapidly, absent the appropriate safeguards.[80] Interconnections could also arise or grow in connection with stablecoin activities if, for example, traditional assets were to be held as part of those activities.[81] In addition, as the FSOC has noted, "[c]rypto-asset trading platforms may also have the potential for greater interconnections by providing a wide variety of services, including leveraged trading and asset custody, to a range of retail investors and traditional financial institutions. Consumers can also increasingly access crypto-asset activities, including through certain traditional money services businesses."[82] Interconnections also exist within and among entities operating in the crypto-asset ecosystem and could accelerate given the recent collapses of firms active in this space and potential acquisitions by rival nonbank firms and exchanges engaged in crypto-related activities.[83]

To monitor potential financial stability risks that could occur from the interconnections and interdependencies between the crypto-asset ecosystem and the traditional financial system, as well as within the crypto-asset ecosystem, authorities should ensure that they have sufficient information to monitor such risks. In some cases, they may need to implement "[a] structured and recurring gathering of quantitative data focused on the nexus between banks and crypto" to "help ensure that regulators have an accurate and complete view of the risk."[84] Authorities also should ensure they have sufficient data or are able to collect such data from nonbank firms and platforms engaged in crypto-related activities about their activities with traditional financial institutions and within the crypto ecosystem itself to enable "more effective surveillance of financial stability risks."[85] International coordination and collaboration, including with respect to data collection and information sharing to monitor financial stability, illicit finance, and other risks, are crucial given the borderless nature of the crypto ecosystem.

9. Authorities should ensure that crypto-asset service providers that combine multiple functions and activities, for example crypto-asset trading platforms, are subject to regulation, supervision and oversight that comprehensively address the risks associated with individual functions as well as the risks arising from the combination of functions, including requirements to separate certain functions and activities, as appropriate.

BPI and TCH agree that all entities in the crypto ecosystem should be subject to regulation, supervision, and oversight that address the risks associated with individual functions in which they engage and the risks associated with the combination of functions.

Consolidated supervision and oversight of a crypto-asset entity and its subsidiaries, affiliates, and, potentially, service providers are important to ensure that the entity as a whole is appropriately

[80] *Id.*

[81] *Id.*

[82] *Id.*

[83] *See* FINANCIAL STABILITY OVERSIGHT COUNCIL, *supra* note 40, at 34–40.

[84] Hsu, *supra* note 74, at 8–9.

[85] *Id.* 9.

managing risks to users, market participants, and to the financial system more broadly.[86] Consolidated supervision is a hallmark of banking supervision and regulation in the United States and addresses the risks of entire organizations. Regulatory coordination is critical in this regard. In some cases, legislation or additional rulemaking may be necessary to provide regulators with the authorities they need to ensure that all crypto-asset entities and their subsidiaries and affiliates are subject to appropriate oversight on an individual and consolidated basis.[87] Requirements should apply on a consolidated basis to ensure that risks are not transmitted within or among crypto entities and do not spill over into the traditional financial system or harm crypto users.

Requirements imposed on the crypto-asset ecosystem under a regulatory and supervisory framework applicable to service providers, trading platforms, and other parties should not create materially different standards from those that apply to similar activities conducted within the regulatory perimeter (e.g., making payments, custodial services, and storing value) because such differences expose consumers, businesses, and investors to risks and engender regulatory arbitrage. This includes the functional separation of key financial activities, such as the provision of safekeeping services, to help mitigate financial stability risk and enhance investor protection. For example, regulators should impose, at a minimum, activity restrictions limiting the vertical integration of functions, appropriate capital and liquidity requirements, separation, segregation, and control requirements for custodial client assets, disclosure requirements, prudential requirements, data and cybersecurity controls, consumer protection mandates, AML/CFT requirements, and supervision, examination, and enforcement.[88]

III. Feedback on the FSB's Proposed Recommendations on Stablecoins

As noted previously, it is important to define key terms and concepts, including what is meant by the term "stablecoins." The GSC Consultative Report defines a stablecoin as "a crypto-asset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets."[89] As we noted at the outset, this definition should not include tokenized commercial bank deposits. Currently, stablecoins are used to trade in and out of crypto assets but could potentially be used as a payment mechanism.[90] In general, a stablecoin issuer commits to sell its stablecoin, and redeem it on demand, at the coin's par value and holds a designated pool of assets to "back" this commitment. In this context, the assets backing the stablecoin need to be available to, or prioritized for, the stablecoin holders who may want to redeem, and the assets cannot be subject to claims of others. This could be accomplished in any number of ways, such as ensuring that:

- stablecoin holders have a priority claim on the assets vis-à-vis other liability holders and that stablecoin redemptions are not subject to a stay in bankruptcy;
- stablecoins are collateralized by the assets; or

[86] *See* FINANCIAL STABILITY OVERSIGHT COUNCIL, *supra* note 40, at 117.

[87] *Id.*

[88] *See id*. Regulators should also impose the restrictions on transactions with affiliates comparable to those that apply to banks in the United States under sections 23A and 23B of the Federal Reserve Act.

[89] GSC CONSULTATIVE REPORT, *supra* note 3, at 73.

[90] *See* REPORT ON STABLECOINS, *supra* note 27.

- assets are held in trust for the stablecoin holders and are not assets of the stablecoin issuer.

The pool of assets is supposed to consist of safe, liquid assets, such as government securities (e.g., U.S. Treasury bills) and insured bank demand deposits, which could be used to meet many redemptions with high confidence. In practice, however, some of the assets currently held by some of the largest stablecoin issuers, which they refer to as their "reserves," are in fact less liquid and riskier assets, like commercial paper and corporate bonds.[91] These and other differences have led to three general types of stablecoins being available today, as described in Appendix C.

Today's largest stablecoin issuers include Tether (USDT), Circle (USDC), and Paxos (USDP), though the contents of their pools of assets vary greatly. As noted previously, we use the term "stablecoin" in this letter to refer to nonbank-issued stablecoins and not to tokenized or blockchain-based bank deposits.

Stablecoin Arrangements Have Grown Rapidly and Present Numerous Risks

Nonbank stablecoin issuers and arrangements have proliferated in the eight years since the first stablecoin was issued.[92] Along with this proliferation has come a multitude of significant risks, as outlined above. These include financial stability risks that the disruption or failure of a stablecoin arrangement could pose. Although no single stablecoin arrangement has yet achieved the size and scale to pose such a risk, BPI and TCH agree with the FSB's assessment that a global stablecoin with reach and adoption across multiple jurisdictions and substantial volume could pose financial stability risks. Robust, consistent oversight of stablecoins by governments across the globe will enhance financial stability and help ensure that financial systems are protected from the risk presented by systemically important stablecoin arrangements.

Stablecoin arrangements differ, at least in the United States, from existing payments systems. Among the latter, even non-systemically important systems have meaningful regulatory and supervisory frameworks that apply.[93] Because there is no comprehensive existing regulatory and supervisory

---

[91] Although it has become somewhat commonplace to refer the pool of assets backing a stablecoin coin as "reserves," we avoid that term because so-called "reserves" in the stablecoin context serve a different function from, and consist of different assets than, reserves that ordinary banks can be required to hold as a percentage of their deposit accounts, as discussed in more detail in Appendix C.

[92] The first stablecoins were issued in 2014. *See* Anastasia Melachrinos & Christian Pfister, *Stablecoins: A Brave New World?*, 4 STANFORD JOURNAL OF BLOCKCHAIN LAW & POLICY 264, 268 (2021). According to U.S. government agencies, as of October 2021, "[t]he market capitalization of stablecoins issued by the largest stablecoin issuers exceeded $127 billion"—a "nearly 500 percent increase over the preceding twelve months." REPORT ON STABLECOINS, *supra* note 27, at 7. Just three stablecoins—Tether (USDT), USD Coin (USDC), and Binance USD (BUSD)—collectively represented more than $156 billion in market capitalization as of November 30, 2022. *See* CoinMarketCap.com, *supra* note 12 (providing market capitalization figures for major crypto assets).

[93] *See, e.g.,* Bank Service Company Act, 12 U.S.C. § 1861, *et. seq*. It should be further noted that supervisory oversight may also extend to such payment systems as a consequence of the regulatory approval national banks may need in order to invest in them. *See* 12 C.F.R. § 5.36.

framework for stablecoins in the United States,[94] or in many other jurisdictions, and because stablecoin arrangements have the ability to scale rapidly and generally can be transferred without regard to international borders, it is important that comprehensive requirements addressing all the risks that stablecoins could pose be implemented as soon as possible so the framework is in place if and when one or more stablecoins become systemically important.[95] Only through such proactive action can the regulatory community ensure that the financial system will be adequately protected.

One way that a stablecoin could be offered without undermining the banking system would be for stablecoins to be designed to be equivalent to bank deposits. In the United States, under existing federal and state law, banks are authorized to issue tokenized deposits, establish blockchain-based deposit accounts, and issue stablecoins, provided they do so in a safe and sound manner.[96] There is no federal legal framework governing the issuance of stablecoins by nonbanks, however.[97] Should such a

[94] Some states in the United States with laws and regulations crafted for payments services, such as money-transmitter licensing laws/regulations, might apply those laws/regulations to stablecoins, particularly where stablecoins are provided to consumers and can serve as a means of payment. *See* Danny Nelson, *FinCEN: Stablecoin Issuers Are Money Transmitters, No Matter What*, COINDESK (Nov. 19, 2019) (link) (noting that then-FinCEN Director Kenneth opined that stablecoin issuers are money transmitters when they function as such). In addition, some states have begun implementing special licensing requirements that apply to digital-currency–focused money transmission businesses, potentially including certain types of stablecoin arrangements. *See, e.g.,* New York State Department of Financial Services, *Virtual Currency Businesses* (link); Nevada Financial Institutions Division, *Nevada Financial Institutions Division Statement on Regulation of Cryptocurrency in Nevad*a (Aug. 19, 2019) (link); Wyoming Division of Banking, *Special Purpose Depository Institutions* (link) (detailing state laws and regulations that might be applied to stablecoin arrangements depending on the characteristics and function of those arrangements). Still, money transmission regulation is quite different from prudential bank regulation, as recently observed by Acting Comptroller of the Currency Michael J. Hsu. *See* Hsu, *supra* note 26, at 4.

[95] *See, e.g.,* REPORT ON STABLECOINS, *supra* note 27, at 2 (noting "there are key gaps in prudential authority over stablecoins used for payments purposes").

[96] *See, e.g.*, Office of the Comptroller of the Currency, *OCC Chief Counsel's Interpretation on National Bank and Federal Savings Association Authority to Use Independent Node Verification Networks and Stablecoins for Payment Activities*, Interpretive Letter No. 1174 (Jan. 4, 2020) (link). *See also* TCH, Bank Issuance of Stablecoins and Related Services: Legal Authority and Policy Considerations (Nov. 2022) (link) (provided by Sullivan & Cromwell LLP at TCH's request).

[97] The protection of U.S. digital asset users, including businesses and consumers, and the financial system from the risks associated with digital assets, including cryptocurrency and stablecoins, is far too important to leave to a patchwork of state money transmitter laws that may or may not apply depending on the vagaries of state statutes, individual state interpretations, and developing state regulatory schemes. *See* Judith Rinearson et al. *Trouble in Paradise: Florida Court Rules That Selling Bitcoin Is Money Transmission*, (K&L Gates LLP, U.S. FinTech Alert, Feb. 13, 2019) (link) (noting that some states have "amended their money transmitter statutes to include or exclude virtual currencies explicitly"). *See also* Pennsylvania Department of Banking, Money Transmitter Act Guidance for Virtual Currency Businesses (Jan. 23, 2019) (link) (noting that because virtual currency is not "currency or legal tender" it is not covered by Pennsylvania's Money Transmitter Act); California Department of Financial Protection and Innovation, Interpretive Opinion (Nov. 3, 2022) (link) (indicating that the California Department of Financial Protection and Innovation would not require a crypto exchange to obtain a license under its Money Transmission Act). *Cf.* New York State Department of Financial Services, Virtual Currency Guidance (June 8, 2022) (link) (constituting guidance to BitLicense holders and New York-chartered limited-purpose trust companies that issue U.S. dollar-backed stablecoins and focusing on NYDFS requirements relating to the redeemability of stablecoins, the assets backing those coins, and attestations about the assets that back those coins).

framework for nonbank issuers be developed, it should be developed on a home-country basis (at the national level) and be designed to promote a safe, healthy, and competitive U.S. stablecoin system. Additionally, it should prioritize the safety, soundness, and resiliency of the stablecoin issuer; the protection of consumers; the preservation of U.S. financial stability; the prevention of financial crimes and illicit finance; and the assurance that stablecoin issuers can be resolved in a safe and orderly way if they become troubled and fail. Refer to Appendix D for BPI and TCH's recommendations on the fundamental issues a stablecoin legal framework in the United States should address.

A recent Federal Reserve research paper considered a model in which stablecoins were backed by commercial bank deposits that were used for fractional reserve banking.[98] It concluded that bank intermediation would not be disrupted so long as "the treatment of stablecoin deposits [were] the same as non-stablecoin deposits in terms of the required reserve ratio, liquidity coverage and other regulatory and self-imposed risk limits."[99] The paper clarified that, in such a model, "the stablecoin issuers [would] rely on commercial bank deposits as assets, and the commercial banks [would] practice fractional reserve banking with the stablecoins and/or stablecoin deposits, meaning the stablecoins [would be] ultimately backed by a mix of loans, assets, and central bank reserves."[100] In order for there to be true equivalency, the stablecoin deposits would need to be insured and subject to similar treatment as other deposits in terms of insurance premiums.[101] This design would seem to align with the public sector's expectations for appropriate regulation of stablecoins. The PWG, FDIC, and OCC recommended that only insured depository institutions be permitted to issue stablecoins.[102] Stablecoins issued by insured depository institutions could also be available to fund bank lending. Thus, consumers and businesses would retain the convenience that comes with using a stablecoin, and consumer and commercial lending would continue apace. At the same time, there are significant developments underway to expand real-time, 24/7 payments—which could provide similar convenience and other benefits as retail payments stablecoins—and the use of P2P services, such as PayPal, Zelle, and Venmo, continues to grow.

The rapid growth of stablecoin arrangements, their possible use as a payment mechanism, the transfer function associated with them, and the lack in many jurisdictions of a meaningful regulatory and supervisory framework that applies to them present unique risks to the financial system. TCH has previously expressed support for the full application of the PFMI to stablecoin arrangements, which would be an important step in addressing the risks presented by those arrangements on a global basis, as the FSB acknowledges in the GSC Consultative Report.[103] The FSB's recommendations would further help set uniform expectations for governments to monitor and address the risks posed by stablecoins.

---

[98] *See* Gordon Y. Liao & John Caramichael, *Stablecoins: Growth Potential and Impact on Banking*, International Finance Discussion Papers 1334 (Board of Governors of the Federal Reserve System, Jan. 2022) (link).

[99] *Id.* at 14.

[100] *Id*. at 13.

[101] *See id*. at 14, n.30.

[102] *See* REPORT ON STABLECOINS, *supra* note 27, at 17.

[103] *See* APPLICATION OF THE PRINCIPLES FOR FINANCIAL MARKET INFRASTRUCTURES TO STABLECOIN ARRANGEMENTS: CONSULTATIVE REPORT, *supra* note 59; Letter from Robert C. Hunter to Committee on Payments and Market Infrastructures & Board of the International Organization of Securities Commissions, *supra* note 59. *See also* GSC CONSULTATIVE REPORT, *supra* note 3, at 8.

The FSB's recommendations would apply only to global stablecoin ("GSC") arrangements, defined according to three characteristics that distinguish a GSC from other crypto-assets and other stablecoins. Those characteristics are (i) the existence of a stabilization mechanism, (ii) usability as a means of payment and/or as a store of value, and (iii) the potential reach and adoption across multiple jurisdictions. The first two characteristics (the existence of a stabilization mechanism and usability as a means of payment and/or store of value)—and the unique risks that these characteristics pose—distinguish stablecoins from other crypto assets. The third—the potential reach and adoption across multiple jurisdictions—differentiates GSCs from other stablecoins according to the FSB. Although TCH and BPI support the application of the FSB's recommendations to GSCs, which present particular cross-border risks under the FSB's GSC definition, we believe further that *all* payment stablecoin arrangements should be subject to robust regulation and oversight on a home-country basis given their cross-border nature and ability to scale quickly. Mitigating potential risks from the inception of such arrangements is therefore important.

Finally, in some jurisdictions, some nonbank entities engaged in, or seeking to engage in, stablecoin issuance and entities with banking charters that do not have deposit insurance and are not subject to consolidated federal supervision have sought access to central bank reserves. In the United States, and likely in many other jurisdictions, there are many benefits that an account at the central bank provides, including being able to clear and settle transactions without liquidity or credit risk, access to emergency borrowing, and a suite of other services. These features are core elements of a nation's financial and monetary system and therefore demand the highest protection against risk.

In the United States, access to central bank accounts and services is limited by federal statute. The Federal Reserve Board recently adopted guidelines governing the consideration of applications for access to master accounts at Federal Reserve Banks.[104] In proposing the guidelines, the Federal Reserve Board explained that the "proposed account access guidelines are centered on a foundation of risk management and mitigation. In developing the proposed guidelines, the Board considered the risks that may arise when an institution gains access to accounts and services. These risks include, among others, risks to the Reserve Banks, to the payment system, to the financial system, and to the effective implementation of monetary policy."[105]

The Federal Reserve Board thus adopted a tiered framework of increasingly stringent levels of scrutiny and review for entities seeking master accounts, with banking entities with federal deposit insurance and subject to prudential supervision by a federal banking agency at both the institution and holding company level (where relevant) receiving the lowest level of scrutiny and entities lacking deposit insurance and federal regulatory oversight being subject to the strictest scrutiny.[106] Certain state-chartered, uninsured depository institutions formed for a limited purpose, such as issuing stablecoins or facilitating other crypto-related activities, would fall in this latter category. Nonbank entities, which lack a banking license and which are not subject to the same degree of regulation and supervision as banks,

[104] *See* Guidelines for Evaluating Account and Services Requests, 87 Federal Register 51099 (Aug. 19, 2022) (link).

[105] Proposed Guidelines for Evaluating Account and Services Requests," 86 Federal Register 25865, 25866 (May 11, 2021) (link).

[106] *See* Guidelines for Evaluating Account and Services Requests, 87 Federal Register at 55109–10.

present similar, if not greater, risks as institutions subject to the strictest scrutiny under the Federal Reserve Board's guidelines.

Not limiting account access to appropriately regulated entities could pose significant risk to not only the U.S. financial system but also to the global financial system given the significant interconnections between the private sector and central banks and among central banks themselves. Other jurisdictions should also consider providing central bank accounts only to those entities that are subject to robust supervision and regulation. This would help protect financial institutions and the financial system more broadly from risks posed by unregulated or lightly regulated entities.

There would be other considerable risks associated with granting certain nonbank stablecoin issuers and other less-regulated entities unfettered access to central bank reserves were they to issue stablecoins backed fully by deposits at the central bank. Those reserves could be perceived as the ultimate safe asset in times of economic or market stress and could lead to massive outflows of deposits in the banking system into that issuer's stablecoin, further exacerbating stress on the country's banks, causing them to cut credit lines and pull back from lending precisely at a time when those functions are needed most by the real economy.

If investors shifted into these stablecoins in stress periods, the central bank might need to replace the lost funding by lending large sums to banks and nonbank financial institutions, while purchasing correspondingly large amounts of government and private securities. It would also need to determine which loans or securities to buy—an inherently political decision and an unprecedented role for a central bank in any democracy. This assumes that regulation would remain static, and a crisis like this would be allowed to unfold.

Alternatively, companies could be prohibited from issuing short-term debt—as they might not be able to roll it over in crisis—and banks could be prohibited from funding loans with deposits, as those deposits would no longer represent stable funding. Thus, banks would be required to shift to funding with long-term debt or equity, effectively ending their core economic role of maturity transformation. Borrowing costs for businesses and consumers would increase dramatically, as their loans would no longer be funded by low-cost deposits but rather by equity or long-term debt. The result would be a much smaller U.S. economy, permanently lower long-term economic growth, and a permanently higher unemployment rate. The monetary policy consequences of allowing nonbank stablecoin issuers or other less-regulated entities direct access to central bank reserves are difficult to exaggerate.

Because central banks, including the Federal Reserve, conduct monetary policy by providing reserve balances to depository institutions, the massive volatility in reserve balances potentially caused by swings in global demand for stablecoins could create substantial uncertainties for the implementation of monetary policy. To mitigate that uncertainty, central bank balance sheets would likely have to be much larger than they are now.

There also could be foreign policy effects that have not yet been entirely explored. Emerging markets experiencing economic hardship might expect their citizens to go to offshore exchanges to buy stablecoins backed by central bank reserves, thereby eliminating all their credit and liquidity risk but potentially destabilizing local economies. It is unclear whether export controls could prevent such a phenomenon from occurring. Given uncertainties in AML/CFT and sanctions enforcement, it is unclear whether such transactions would occur in the dark. The foreign policy ramifications of offering riskless

central bank reserves to anyone, regardless of nationality, are difficult to fathom. Thus, nonbank stablecoin issuers and uninsured and non–federally regulated banks should not be granted access to central bank reserves, including at the Federal Reserve.[107]

The FSB should make clear that local authorities should require all stablecoin arrangements to abide by the home country's regulatory framework, including requirements implemented pursuant to the FSB's principles. A key risk associated with stablecoin arrangements is their ability to scale rapidly.[108] This is due to network effects and can be influenced by relationships between stablecoin issuers and existing user bases or platforms. As such, it is critical that all arrangements be subject to a robust regulatory framework at their inception so they do not become a threat to financial stability later. Even if a stablecoin does not reach GSC scale, consumers and investors, as well as financial institutions, could be harmed. Local authorities should address this risk through the application of robust requirements to those arrangements.

BPI and TCH therefore support the FSB recommendations outlined below and recommend further that local authorities apply these recommendations to *all* stablecoin arrangements, not just to GSCs.

1. **Authorities should have and utilize the necessary or appropriate powers and tools, and adequate resources, to comprehensively regulate, supervise, and oversee a GSC arrangement and its associated functions and activities, and enforce relevant laws and regulations effectively.**

BPI and TCH support this recommendation. As noted, stablecoins, depending on what form they take, present various risks to consumers and investors. If they were to grow at scale, they could threaten financial stability if their risks are not appropriately addressed. Because the activities and functions in a stablecoin arrangement may be distributed across various parties, a prudential framework that focuses exclusively on stablecoin issuers is unlikely to adequately address payment system risks.[109] To ensure that stablecoin arrangements are subject to a comprehensive regulatory framework, authorities should have the ability to "require any entity that performs activities critical to the functioning of the stablecoin arrangement to meet appropriate risk-management standards, such as the Principles for Financial Market Infrastructures as adapted to stablecoin arrangements."[110] Authorities should have the appropriate powers to regulate and supervise the market operations nonbank stablecoin issuers undertake to help ensure the stability of their coins' value.

---

[107] See Appendix C for a discussion of the Federal Reserve Board's concerns with pass-through investment entities ("PTIEs"), including banks, that seek to hold virtually all their assets in the form of balances at Federal Reserve Banks. The Federal Reserve Board explained that PTIEs could negatively affect financial stability by attracting deposits during times of stress, which would divert funding away from nonfinancial firms, financial institutions, and state and local governments, and also expressed concern that a proliferation of PTIEs could magnify these effects across the financial system.

[108] REPORT ON STABLECOINS, *supra* note 27, at 14.

[109] *See id.* at 16–17. The parties involved in a stablecoin arrangement can include (1) those involved in its creation, (2) those involved in transfers between holders, and (3) those involved in storing coins. This makes arrangements highly distributed and complex.

[110] *Id.* at 17 (footnote omitted).

To accomplish consolidated, comprehensive regulation and supervision of stablecoin arrangements, authorities should, as the FSB has suggested, "identify and address any significant gaps in their regulatory, supervisory and oversight frameworks through changes in regulations, or policy, as appropriate. In some jurisdictions, legislative changes may be necessary or appropriate to address those gaps. Authorities should have the powers and capabilities to enforce applicable regulatory, supervisory and oversight requirements, including the ability to undertake inspections or examinations, and, when necessary or appropriate, require corrective actions and take enforcement measures."[111]

2. Authorities should apply comprehensive regulatory, supervisory and oversight requirements consistent with international standards to GSC arrangements on a functional basis and proportionate to their risks insofar as such requirements are consistent with their respective mandates.

BPI and TCH agree with this recommendation, as custodial wallet service providers and trading platforms present risks that should be addressed through appropriate oversight.

As the GSC Consultative Report explains, this recommendation and the changes made to it since it was first issued in 2020 are "intended to identify wallets and trading services more clearly, and clarify that custodial wallet service providers and trading platforms associated with GSC activities should be subject to regulation, supervision and oversight."[112] In the United States, the PWG, FDIC, and OCC observed that the failure or distress of a stablecoin issuer or a wallet provider could adversely affect financial stability and the real economy and that the combination of a stablecoin issuer or wallet provider and a commercial firm could lead to an excessive concentration of economic power.[113] They also concluded that "[g]iven the central role that custodial wallet providers play within a stablecoin arrangement, and the risks attendant to the relationship between custodial wallet providers and stablecoin users, Congress should require custodial wallet providers to be subject to appropriate federal oversight. Such oversight should include authority to restrict these service providers from lending customer stablecoins, and to require compliance with appropriate risk-management, liquidity, and capital requirements. In addition, to address concerns about concentration of economic power, Congress should consider other standards for custodial wallet providers, such as limits on affiliation with commercial entities or on use of users' transaction data."[114] We agree.

3. Authorities should cooperate and coordinate with each other, both domestically and internationally, to foster efficient and effective communication, information sharing and consultation in order to support each other in fulfilling their respective mandates and to ensure comprehensive regulation, supervision, and oversight of a GSC arrangement across borders and sectors.

---

[111] GSC CONSULTATIVE REPORT, *supra* note 3, at 11.

[112] *Id*.

[113] *See* REPORT ON STABLECOINS, *supra* note 27, at 14.

[114] *Id.* at 17.

BPI and TCH support this recommendation and, as described previously, have advocated for a coordinated, whole-of-government approach that would help protect consumers and investors and the U.S. financial system while allowing for responsible development of digital assets and digital-asset ecosystems.

Digital assets have the potential to provide benefits to consumers and businesses and to the financial system. Nevertheless, because of the potential risks presented by digital assets, including stablecoins, it would be prudent to have a coordinated, comprehensive, government-wide approach in local jurisdictions to evaluate the potential benefits and risks of digital assets and to establish a regulatory framework to address the risks they do pose. A fractured approach to evaluation would likely result in the failure to establish an appropriate, comprehensive regulatory framework for digital assets and related activities, including stablecoin activities, which could ultimately harm customers and, potentially, the financial system. The risks of an uncoordinated approach to the regulation of digital assets and related activities include regulatory arbitrage, which could allow risks to build up outside the view of any governmental authority and thereby threaten financial stability and result in consumer and investor harm. Because of the borderless nature of crypto assets, including stablecoins, coordination across borders is critical to comprehensively address the risks they present and to eliminate opportunities for regulatory arbitrage. This coordination is particularly important with respect to ensuring that stablecoin arrangements meet appropriate AML/CFT requirements.

4. Authorities should require that GSC arrangements have in place a comprehensive governance framework with clear and direct lines of responsibility and accountability for all functions and activities within the GSC arrangement.

BPI and TCH support this recommendation and agree with the FSB that the decentralized nature of certain digital assets entities, including stablecoin arrangements, "may make it difficult to apply relevant policies and standards effectively and to identify entities and persons that can be held accountable for their effective implementation."[115]

The FSOC has identified governance and decision making breakdowns as a possible source of shocks in the crypto-asset ecosystem, and the PWG, FDIC, and OCC highlighted that payment stablecoins "face many of the same basic risks as traditional payment systems, including credit risk, liquidity risk, operational risk, risks arising from improper or ineffective system governance, and settlement risk" but that "unlike traditional payment systems where risk is managed centrally by the payment system operator, some stablecoin arrangements feature decentralized decision-making and complex operations where no single organization is responsible or accountable for risk management and resilient operation of the entire arrangement."[116]

Therefore, requiring stablecoin arrangements to have a comprehensive governance framework, with clear and direct lines of responsibility, is important to ensure accountability for managing all functions and activities within a stablecoin arrangement. BPI and TCH note further that a financial market infrastructure's governance arrangements are critical to protecting the safety and efficiency of

[115] *See* GSC CONSULTATIVE REPORT, *supra* note 3, at 14.

[116] *See* FINANCIAL STABILITY OVERSIGHT COUNCIL, *supra* note 40, at 72–73; REPORT ON STABLECOINS, *supra* note 27, at 12–13.

the financial market infrastructure, supporting the stability of the broader financial system, other relevant public interest considerations, and the objectives of relevant stakeholders. Clear and effective governance is also essential to meeting a board's responsibility to establish and oversee a clear, documented risk management framework.[117]

5. **Authorities should require that GSC arrangements have effective risk management frameworks in place especially with regard to operational resilience, cyber security safeguards and AML/CFT measures, as well as "fit and proper" requirements, if applicable, and consistent with jurisdictions' laws and regulations.**

BPI and TCH support this recommendation.

As noted, stablecoin arrangements can present numerous risks. It is therefore important that these arrangements have effective risk management frameworks in place to address those risks, including operational, cybersecurity, and money-laundering and terrorist-financing risks. As the PWG, FDIC, and OCC explained, "operational issues in a payment system can disrupt the ability of users to make payments, which can in turn disrupt economic activity."[118] Operational problems that result in a payment error or a fraudulent payment can inflict losses on users.[119] Stablecoin arrangements face these risks and may "face novel operational risks related to the validation and confirmation of stablecoin transactions and the management and integrity of the distributed ledger."[120] In addition, operational risks may "be more difficult to manage or supervise in a stablecoin arrangement, especially when the supporting infrastructure is beyond the control of any one organization (including the entities involved in the stablecoin arrangement) and there is no clear entity to regulate."[121] Nonbank stablecoin issuers often outsource their core recordkeeping when they choose a layer 1 protocol. They should be subject to the same level of risk management requirements to which banks are subject when they outsource core processes to a third party.

As discussed previously, stablecoin arrangements are vulnerable to cyber risks and have suffered massive, sudden shocks due to internal and external manipulation and attack, including cyberattack. Regulators should ensure that data protection and cybersecurity requirements and expectations are consistently applied to all entities engaging in stablecoin-related activities. BPI and TCH have long warned of the dangers of uneven expectations and requirements regarding consumer data protections and cybersecurity controls for banks versus nonbank fintechs.[122] Banks and other regulated entities have developed sophisticated systems to protect consumer data and to detect, prevent, and respond to cyber threats. As described previously, banks and other regulated entities are generally subject to extensive regulatory oversight to ensure such protections are in place and can face

---

[117] *See* APPLICATION OF THE PRINCIPLES FOR FINANCIAL MARKET INFRASTRUCTURES TO STABLECOIN ARRANGEMENTS: CONSULTATIVE REPORT, *supra* note 59, at 13.

[118] REPORT ON STABLECOINS, *supra* note 27, at 13.

[119] *Id.*

[120] *Id.*

[121] *Id.*

[122] Refer to footnote 50 for a list of citations.

financial penalties or restrictions on their activities if they fail to comply with their obligations. Furthermore, banks, unlike nonbanks, are subject to regular examination and supervision.

As discussed throughout this letter, crypto-asset–related transactions present various illicit finance and national security risks. The primary "illicit financing risks associated with virtual assets come from gaps in implementation of the international AML/CFT standards across countries; the use of anonymity-enhancing technologies; the lack of covered financial institutions as intermediaries—and thus the absence of AML/CFT controls—in some virtual asset transactions; and [virtual asset service providers ("VASPs")] that are non-compliant with AML/CFT and other regulatory obligations."[123] This is even more concerning when, as the U.S. Treasury Department noted, "stablecoins and other digital assets can be used to transfer large amounts of value across borders very quickly. A rapid increase in cross-border payments could amplify ML/TF risks due to the uneven implementation of global international AML/CFT standards developed by the [Financial Action Task Force]."[124] To mitigate these risks, "international standards for the regulation and supervision of service providers associated with stablecoins and other digital assets [should be] effectively implemented worldwide."[125] Gaps in regulation among different countries could allow Illicit actors to "exploit these gaps by using services in countries with weak regulatory and supervisory regimes to launder funds, store proceeds of crime, or evade sanctions in stablecoins or other digital assets."[126]

Both BPI and TCH have responded to the U.S. Treasury Department's proposed action plan to address illicit financing risks of digital assets[127] and have previously commented on ways in which the federal government could mitigate risks associated with digital assets.[128] BPI and TCH have recommended that the Treasury Department, working with other relevant offices and agencies of the U.S. government, ensure the following principles and steps are considered in developing regulations and taking other actions designed to mitigate the illicit finance risks that digital assets and digital-asset transactions pose:

1. The requirements and expectations in respect of AML and CFT activities should be consistent for all institutions that engage in equivalent activities with similar illicit finance risk characteristics, regardless of a particular entity's status as a bank, money services business, or other type of institution.
2. The Treasury Department should recognize and take actions to mitigate the illicit finance risks associated with specific digital assets and digital-asset transactions, such as risks relating to reduced transparency and visibility for law enforcement, disintermediation of financial institutions subject to the BSA, and increased complexity.

---

[123] *See* ACTION PLAN TO ADDRESS ILLICIT FINANCING RISKS OF DIGITAL ASSETS, *supra* note 22, at 4.

[124] REPORT ON STABLECOINS, *supra* note 27, at 19.

[125] *Id.*

[126] *Id.*

[127] *See* Letter from Philip Keitel to U.S. Department of the Treasury (Nov. 3, 2022), *supra* note 38; Letter from Gregg Rozansky to Jon Fishman (Nov. 3, 2022), *supra* note 38.

[128] *See* Letter from Angelena Bradfield to Financial Crimes Enforcement Network, *supra* note 54; Letter from Robert C. Hunter to Financial Crimes Enforcement Network, *supra* note 54.

3. U.S. authorities should continue their efforts to implement the AML Act. These efforts, including facilitation of the AML Act's statutory purposes of reinforcing the risk-based nature of financial institution AML programs and encouraging technological innovation in AML compliance, will be important to mitigate illicit finance risks posed by digital assets and digital-asset transactions.
4. The U.S. Treasury Department should facilitate cross-border cooperation and other information sharing relating to the illicit finance risks of digital assets and digital-asset transactions.

BPI and TCH recommend that equivalent regulators in other countries consider adopting the same principles and taking the same steps to the extent they have not already done so.

6. Authorities should require that GSC arrangements have in place robust systems and processes for collecting, storing, and safeguarding data.

BPI and TCH support this recommendation and have long warned of the dangers of uneven expectations and requirements regarding consumer data protections and cybersecurity controls for banks versus nonbank fintechs.[129]

As discussed previously, banks and other regulated entities have developed sophisticated systems to protect consumer data and to detect, prevent, and respond to cyber threats. Banks and other regulated entities are generally subject to extensive regulatory oversight to ensure such protections are in place and can face financial penalties or restrictions on their activities if they fail to comply with their obligations. For example, U.S. banks are subject to the Gramm–Leach–Bliley Act and its implementing regulations, which obligate them to safeguard their consumer customers' information, extensive IT guidance from the FFIEC,[130] and third-party risk management guidance from the federal banking agencies.[131] As noted, banks, unlike nonbanks, are subject to regular examination and supervision. To ensure that data is adequately protected, nonbank stablecoin issuers should be subject to the same requirements and expectations and to regular, direct supervision and examination to ensure compliance with those requirements and expectations.

7. Authorities should require that GSC arrangements have appropriate recovery and resolution plans.

BPI and TCH agree that, given the opacity and uncertainty that currently surround the potential failure of a stablecoin arrangement and the related rights of various parties and applicability of existing resolution frameworks, it is important that stablecoin arrangements have robust, comprehensive recovery and resolution plans to provide clarity on the rights of investors, consumers, and other relevant

[129] Refer to footnote 50 for a list of citations.

[130] As noted previously (see footnote 51), 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.

[131] See footnote 52 for a brief description of that guidance and for a citation to a joint proposal by the federal banking agencies to update it.

stakeholders. These plans should include clear disclosure about the redemption rights of stablecoin holders.

8. Authorities should require that GSC issuers provide all users and relevant stakeholders with comprehensive and transparent information to understand the functioning of the GSC arrangement, including with respect to governance framework, redemption rights, and its stabilization mechanism.

BPI and TCH support this recommendation.

As discussed previously, consumers, investors, and businesses must have a clear understanding of the benefits and risks of digital assets, as well as an understanding of how digital assets differ from traditional products and payment instruments and rails so they can make informed decisions. While some nonbank firms engaged in crypto-related activities in the United States are subject to state money transmitter licensing schemes, these frameworks are insufficient to address these issues and risks.[132] Instead, new laws, or revisions to existing laws, are necessary to ensure that appropriate consumer protections and transaction risk allocation are in place. Such entities should operate with business models that enable them to absorb potential losses. Ensuring that consumers, investors, and businesses can make informed decisions may also require guardrails be put in place to enable them to identify when longstanding sources of protection, such as deposit insurance, exist or apply and when they do not.

As discussed previously, "[m]any nonbank firms in the crypto-asset ecosystem have advertised themselves as regulated" even though they are generally not subject to "a comprehensive framework for mitigating financial stability vulnerabilities arising from other activities" such as those conducted by "a trading platform or stablecoin issuer."[133] Some crypto-asset entities have made false or misleading statements about the availability of federal deposit insurance, leading customers to falsely believe that they were protected by the government safety net.[134] Crypto-asset firms have misrepresented how they are regulated, which made consumers and investors uncertain whether a given crypto-asset product was regulated to the same extent as other financial products.[135]

Thus, regulators must require and enforce robust, accurate disclosures by entities in the crypto ecosystem. Such disclosures must include disclosures about their operations, risk profiles, financial condition, conflicts of interest, the products they provide and activities they conduct, the regulatory oversight to which they are subject, transactions with affiliates, and any government safety net to which they may have resort. Nonbank stablecoin issuers should be transparent about the commercial arrangements they have with, among others, market makers, VASPs, and layer 1 protocol network providers. Nonbank stablecoin issuers should also be required to disclose how they hold the assets "backing" their coins (e.g., with a third-party custodian, asset manager, etc.).

---

[132] See footnote 26 for an explanation of why these frameworks are inadequate.

[133] *See* Fact Sheet, The Financial Stability Oversight Council's Report on Digital Asset Financial Stability Risks and Regulation, *supra* note 77 at 2.

[134] *Id.*

[135] *Id*.

Robust and accurate disclosures are critical to help crypto-asset users meaningfully consider the risks presented by crypto-asset products and services and make informed decisions as to whether or to what extent to engage in the crypto-asset ecosystem.

9. Authorities should require that GSC arrangements provide a robust legal claim to all users against the issuer and/or underlying reserve assets and guarantee timely redemption. For GSCs referenced to a single fiat currency, redemption should be at par into fiat. To maintain a stable value at all times and mitigate the risks of runs, authorities should require GSC arrangements to have an effective stabilization mechanism, clear redemption rights and meet prudential requirements.

BPI and TCH agree with this recommendation.

Stablecoin arrangements "could serve as a reliable means of payment or store of value only when there is confidence in its value, particularly in periods of stress. For stablecoins, this confidence could arise in part from its redeemability, and the belief that such redeemability is supported by a stabilization mechanism that will function effectively both during normal conditions and during periods of stress."[136] This confidence could be "undermined by factors including: (1) use of reserve assets that could fall in price or become illiquid; (2) a failure to appropriately safeguard reserve assets; (3) a lack of clarity regarding the redemption rights of stablecoin holders; and (4) operational risks related to cybersecurity and the collecting, storing, and safeguarding of data."[137]

A stablecoin's failure to perform according to expectations could lead to destabilizing runs. Therefore, ensuring robust legal claims for all users, guaranteeing timely redemption, effective stabilization mechanisms, clear redemption rights, and meeting prudential requirements are important to protecting users and the financial system more broadly. BPI and TCH note that, while some U.S. regulatory frameworks (such as the BSA) apply to natural persons, legal persons, *and* unincorporated entities, more optimal regulatory and law enforcement outcomes would result if digital-asset service providers (such as digital asset intermediaries, trading platforms, and accounting platforms or ledgers) that operate with customers located in the United States were required to incorporate in the United States under a given subset of the existing types of legal entity.[138] Requiring providers to have a clear legal personality would also help clarify the contractual remedies available to providers' customers.

[136] REPORT ON STABLECOINS, *supra* note 27, at 12.

[137] *Id.*

[138] *See* FINANCIAL STABILITY OVERSIGHT COUNCIL, *supra* note 40, at 116 (noting there could be "practical challenges to enforcement if market participants are not readily identifiable, or if activities lack linkages with traditional financial institutions or markets that could otherwise facilitate regulatory oversight"). For purposes of this comment, a legal entity is an entity that has legal standing, including the capacity to enter into agreements, assume obligations, incur and pay debts, sue and be sued, and to be held responsible for its actions.

10. **Authorities should require that GSC arrangements meet all applicable regulatory, supervisory and oversight requirements of a particular jurisdiction before commencing any operations in that jurisdiction and adapt to new regulatory requirements as necessary and as appropriate.**

BPI and TCH support this recommendation, but believe all relevant requirements should be met before any stablecoin arrangement commences operations to ensure that consumers, investors, and the financial system are protected from risks.

IV. Conclusion

Digital assets have grown rapidly in recent years. We recognize the potential they have to provide benefits to consumers, businesses, and the financial system. We recognize, too, the risks that certain types of digital assets may present to consumers, businesses, investors, and financial stability. Consequently, it is imperative that meaningful regulatory and supervisory frameworks to address these risks be adopted around the globe. These frameworks should define, and appropriately distinguish, digital assets, cryptocurrencies, and tokenized assets. They should also differentiate between the assets themselves and the technology or infrastructure that underpin them. BPI and TCH support—and the FSB and other public-sector authorities should promote—responsible innovation. Technology like DLT and blockchain may differ in use across functions and activities, as well as in the risks it presents. The frameworks should explicitly clarify that traditional banking products and activities utilizing DLT, blockchain, or other newer technologies are not within their scope. The frameworks should ensure that banks that are subject to comprehensive regulation, supervision, and examination are no less able to engage in digital-asset–related activities than nonbanks. Last, but importantly, the frameworks should apply standards to nonbank digital-asset service providers that are equivalent to those that apply to regulated financial institutions engaged in functionally similar activities.

We thank you for your consideration and review of these comments. If you have any questions or wish to discuss this letter, please do not hesitate to contact us using the contact information provided below.

Very truly yours,

/s// Paige Pidano Paridon

Paige Pidano Paridon
Senior Vice President,
Senior Associate General Counsel
Bank Policy Institute
(703) 887-5229
paige.paridon@bpi.com

/s/ Robert C. Hunter

Robert C. Hunter
Deputy General Counsel & Director of Regulatory and Legislative Affairs
The Clearing House Association L.L.C.
(336) 769-5314
robert.hunter@theclearinghouse.org

Appendix A – Descriptions of the Organizations

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 U.S. Collectively, they employ almost two million Americans, make nearly half of the nation's bank-originated small business loans, and are an engine for financial innovation and economic growth.

The Clearing House Association L.L.C., the country's oldest banking trade association, is a nonpartisan organization that provides informed advocacy and thought leadership on critical payments-related issues. Its sister company, The Clearing House Payments Company L.L.C., owns and operates core payments system infrastructure in the United States, clearing and settling more than $2 trillion each day. See The Clearing House's website at www.theclearinghouse.org.

Appendix B – Illicit Finance Risks Presented by Digital-Asset Technologies and Ecosystems

Mixers/anonymity-enhancing technologies. Governments should explore requiring nonbank providers and developers of digital-asset anonymity-enhancing technologies to include features that maintain records so a clear audit trail can be produced with respect to processed transactions. The Treasury Department's Financial Crimes Enforcement Network ("FinCEN") should also ensure that the nonbank providers and developers of these technologies—or any other future technologies that can similarly be used to enhance anonymity or purposely obscure transaction data—are subject to AML program requirements, compliance expectations, and supervision or oversight consistent with what is imposed on market participants engaged in economically equivalent activities, as banks are required to do.

Digital ledgers. Regulators should consider subjecting the operators of digital ledgers to reporting requirements similar to those applicable to operators of credit card networks in the United States to the extent that they are engaged in a substantially similar function.[139] Doing so would help ensure that regulatory and law enforcement agencies that have resorted to analyzing open blockchains to track transactions among wallets and have employed additional methods to match wallets to actual natural or legal persons are not stymied when a distributed ledger does not provide a complete and transparent record of the transactions among the true wallets involved.

Unhosted wallets. Regulators should consider imposing obligations on banks and money services business to conduct reporting, recordkeeping, and customer verification on certain digital-asset transactions involving an unhosted wallet or other covered wallet. This includes applying the recordkeeping rule for transmittals of funds to transactions between hosted and unhosted wallets and applying the funds-transmittal travel rule to transactions between wallets hosted at VASPs. VASPs must be examined for compliance with both recordkeeping- and travel-rule obligations and be subject, where appropriate, to enforcement actions.[140]

Participants in decentralized finance ("DeFi") projects. In the case of DeFi, the potential lack of legal person or owner status and home jurisdiction of the platform, and the potential lack of transparency as to the natural persons responsible for the platform's creation or maintenance, may hamper any regulatory or law enforcement response. In the case of peer-to-peer payments, increased velocity and cross-border capabilities, as well as the potential for bad actors to more easily access compromised credentials, will affect regulatory and law enforcement responses. Technology companies that develop and support DeFi products and services should be required to collect beneficial ownership information from the users of those products and services.

Ransomware. Ransomware highlights the ways in which virtual assets can present illicit finance risks. Regulators should coordinate to increase transparency and reporting to law enforcement and national security agencies of ransomware events. In doing so, however, they should take care to avoid imposing redundant or otherwise unnecessary compliance burdens on banks and other financial institutions.

---

[139] *See, e.g.,* Anti-Money Laundering Programs for Operators of a Credit Card System, 67 Federal Register 21121, 21127 (Apr. 29, 2002) (link).

[140] *See* FINANCIAL STABILITY OVERSIGHT COUNCIL, *supra* note 40, at 112.

Digital-asset ecosystems in general. Regulators should consider requiring participants in digital-asset transactions to collect information sufficient to develop a complete information trail regarding the originators and beneficiaries of those transactions. Digital assets enable financial transactions to be conducted without involvement of financial institutions subject to the BSA. Regulators should take action to mitigate this disintermediation and the associated illicit finance risks. For example, regulators should clarify how AML program requirements and other obligations, including recordkeeping, apply to DeFi and peer-to-peer payment technologies. Doing so is necessary to further the BSA's purpose of, among other things, requiring reports or records that are "highly useful" for law enforcement and national security agencies.

Specific digital assets and types of digital-asset transactions enable more complexity and raise illicit finance risks. Governments should take steps to recognize and mitigate these risks and to address how existing compliance obligations apply to these digital assets. For example:

Non-fungible tokens (NFTs). NFTs can provide a means for obfuscating the source of crime proceeds, similar to antiquities or art. Accordingly, regulators should treat NFTs as analogous to antiquities and art, including by considering whether NFT markets or persons engaged in NFT transactions should be subject to AML requirements.

Mining pools. Regulators should clarify how financial institutions should view mining pools (groups of cooperating miners who agree to share block rewards in proportion to their contributions) for the purpose of their AML programs.

Private keys. Regulators should provide guidance on how financial institutions should determine the ultimate beneficial owner of a private key. Private keys are strings of characters, similar to passwords, which enable transfers of virtual assets in a particular wallet. In the United States, banks have been granted authority to safeguard private encryption keys (outside the context of crypto assets) and have developed the appropriate risk management processes to do so.[141]

[141] *See* OCC Interpretive Letter No. 1170, *supra* note 47, at 6 (citing OCC Conditional Approval 267, granting a national bank authority to safeguard encrypted keys).

Appendix C – Types of Stablecoins

There are three general types of stablecoins currently. The first type—the so-called "unstable stablecoin"—is backed by assets like corporate debt and asset-backed securities and is thus similar to prime money market funds.[142] These stablecoins present several risks to consumers and the financial system, including the risk of failure, which has occurred, resulting in consumers losing all their money—whether because the underlying assets declined in value or because the money was simply stolen through hacking or defalcation.[143] Second, these stablecoins have been marketed as being backed by "reserves," which, in banking parlance, connotes very safe, liquid assets.[144] In reality, however, these stablecoins are backed by commercial paper—essentially loans.[145] Thus, consumers have been deceived about the safety of these products.[146] If the backing of these stablecoins were called into question, a run could be triggered, with consumers seeking to redeem their stablecoins all at once.[147] Third,

[142] Greg Baer, President & CEO, BPI, Remarks at Women in Housing & Finance Public Policy Lunch, Making Stablecoins Stable: Is the Cure Worse than the Disease? (Sept. 27, 2021) (link).

[143] *See*, *e.g.*, Richi Jennings, *SafeDollar Stablecoin Not Safe Nor Stable: Hack Sends Value to ZERO*, SECURITY BOULEVARD (June 29, 2021) (link); Ryan Browne, *The World's Biggest Stablecoin Has Dropped Below Its $1 Peg*, CNBC (May 12, 2022) (link). *See also The Biggest Threat to Trust in Cryptocurrency: Rug Pulls Put 2021 Cryptocurrency Scam Revenue Close to All-Time Highs*, CHAINALYSIS (Dec. 16, 2021) (finding that over $7.7 billion was stolen in cryptocurrency scams worldwide in 2021) (link).

[144] In the United States, the Federal Reserve Board's Regulation D dictates what may constitute reserves. *See* 12 C.F.R. § 204.5(a)(1) (specifying that depository institutions must satisfy their reserve requirements through vault cash and balances maintained at a Federal Reserve Bank (including, in some instances, those held through a pass-through correspondent)). *See also*, *e.g.,* GLENN R. HUBBARD, MONEY, THE FINANCIAL SYSTEM, AND THE ECONOMY 306 (1994) (explaining that reserves consist of vault cash and banks' deposits with Federal Reserve Banks and that, "[b]ecause of their liquidity, bank holdings of U.S. government securities are sometimes called secondary reserves"); FREDRIC S. MISHKIN, THE ECONOMICS OF MONEY, BANKING, AND FINANCIAL MARKETS 698 (11th ed. 2016) (defining reserves as "[b]anks' holding of deposits in accounts with the Fed plus currency that is physically held by banks (vault cash)"). Likewise, in the Eurosystem, the European Central Bank has mandated that credit institutions hold minimum reserves in the form of balances at accounts at the relevant national central bank. *See* European Central Bank Regulation 2021/378, art. 2(1), 2021 O.J. (L. 73) 1, 3.

[145] *See* Bill Nelson & Paige Pidano Paridon, *Stablecoins Are Backed by 'Reserves'? Give Us a Break*, AMERICAN BANKER (Dec. 10, 2021) (link).

[146] *See* Commodity Futures Trading Commission, "CFTC Orders Tether and Bitfinex to Pay Fines Totaling $42.5 Million," Release No. 8450-21 (Oct. 15, 2021) (link) (noting that "[t]he Tether order finds that since its launch in 2014, Tether has represented that the tether token is a stablecoin . . . [but] that from at least June 1, 2016 to February 25, 2019, Tether misrepresented to customers and the market that Tether maintained sufficient U.S. dollar reserves to back every USDT in circulation with the "equivalent amount of corresponding fiat currency" held by Tether and "safely deposited" in Tether's bank accounts. In fact, Tether reserves were not "fully-backed" the majority of the time.").

[147] *See* REPORT ON STABLECOINS, *supra* note 27, at 12 (highlighting that "[t]he mere prospect of a stablecoin not performing as expected could result in a 'run' on that stablecoin—i.e., a self-reinforcing cycle of redemptions and fire sales of reserve assets. Fire sales of reserve assets could disrupt critical funding markets, depending on the type and volume of reserve assets involved. Runs could spread contagiously from one stablecoin to another, or to other types of financial institutions that are believed to have a similar risk profile. Risks to the broader financial system could rapidly increase as well, especially in the absence of prudential standards.").

because stablecoin issuers in the United States are currently regulated simply at the state level as money service businesses, there is generally no requirement that they disclose what is backing their coins.[148] Fourth, financial stability risk could arise if the failure of a major stablecoin issuer prompted a run on other stablecoin issuers, with those stablecoin issuers forced to liquidate the assets backing their coins. As the PWG, the President, the Secretary of the Treasury, and many other U.S. government officials have outlined, the risks of these instruments must be addressed by appropriate regulation.[149]

The second type of stablecoin—the algorithmic stablecoin—relies on algorithmic measures and/or arbitrage by cryptocurrency traders to maintain its value. Since such stablecoins are not backed by tangible assets, they present significant run risk if investors lose confidence in their stabilization mechanisms, which was illustrated earlier this year when an algorithmic stablecoin lost its dollar peg, triggering a run on crypto assets and erasing over $400 billion in crypto market capitalization practically overnight.[150]

The third type of stablecoin that has been proposed—the so-called "stable stablecoin"—would be backed solely by cash, government securities, repurchase agreements collateralized by government securities, or possibly central bank reserves, which would make it safer than the other two types. Some have proposed that these more stable stablecoins could serve as a payments mechanism. If a stablecoin backed by assets like these were to grow at scale, it could pose the risk that depositors would run *to*, not *from*, it, particularly in times of financial instability, draining the financial system of deposits that would lead to several knock-on effects, including increasing the cost of credit. These concerns are similar to those regarding a U.S. CBDC.

The Federal Reserve Board itself raised such concerns in response to a proposal by TNB USA Inc. ("TNB"), which calls itself The Narrow Bank, to establish a bank with a very narrow business model. Essentially, TNB sought a Federal Reserve Bank master account as a state-chartered institution that would take deposits from institutional investors and invest most of the funds in reserve balances at a Federal Reserve Bank. The interest TNB would earn on those reserve balances would be passed on to TNB's depositors, less a haircut for TNB. TNB has not yet received a master account. The Federal Reserve Board further highlighted its concerns with this type of pass-through investment entity ("PTIE"), noting that "by maintaining all or substantially all of their assets in the form of balances at Reserve Banks and having the ability to attract very large quantities of deposits at a near-[interest on reserves] rate, [PTIEs] have the potential to complicate the implementation of monetary policy . . . [and] could disrupt financial intermediation in ways that are hard to anticipate, and could also have a negative effect

[148] *See generally* Dan Awrey, *Bad Money*, 106 CORNELL LAW REVIEW 1 (2020).

[149] *See, e.g.*, REPORT ON STABLECOINS, *supra* note 27, at 2; Executive Order No. 14067, Ensuring Responsible Development of Digital Assets, 87 Federal Register 14143 (Mar. 14, 2022) (link); Janet L. Yellen, Secretary of the Treasury, Remarks on Digital Assets at American University's Kogod School of Business Center for Innovation (Apr. 7, 2022) (link).

[150] *See* Alexander Osipovich & Caitlin Ostroff, *Crash of TerraUSD Shakes Crypto. 'There Was a Run on the Bank,'* WALL STREET JOURNAL (May 12, 2022); Andrew R. Chow, *The Real Reasons Behind the Crypto Crash, and What We Can Learn from Terra's Fall*, TIME (May 17, 2022).

on financial stability."[151] The Federal Reserve Board explained that PTIEs could negatively affect financial stability by attracting deposits during times of stress, which would divert funding away from nonfinancial firms, financial institutions, and state and local governments.[152] In addition, the Federal Reserve Board explained that a "proliferation of similar PTIEs could magnify these effects across the financial system."[153]

Thus, to the extent so-called stable stablecoins are permitted to be issued in a jurisdiction, local authorities ought to give serious consideration, in evaluating the requirements to which they should be subject, to the risks they pose to financial stability.

[151] Regulation D: Reserve Requirements of Depository Institutions, 84 Federal Register 8829, 8830 (Mar. 12, 2019) (advanced notice of proposed rulemaking) (link).

[152] *Id.* at 8831.

[153] *Id*. at 8830.

Appendix D – U.S. Stablecoin Legal Framework

At a minimum, a stablecoin legal framework for the United States should address:

- *Capital requirements*. Nonbank issuers should be subject to robust capital requirements. Ordinary banks must comply with four regulatory capital ratios, including three risk-based requirements and a tier 1 leverage ratio requirement of 4 percent to be adequately capitalized and 5 percent to be well capitalized. The largest banks are also subject to a supplementary leverage ratio of 6 percent to be deemed well capitalized. Banks with less than $10 billion in assets are allowed to replace the four capital requirements with a 9 percent tier 1 leverage ratio requirement under the community bank leverage ratio framework. While one could argue that these requirements are far too high, there is no argument for applying a lower requirement to nonbank issuers of stablecoins than would apply to banks. Moreover, the largest issuers of stablecoins should be subject to regular stress tests to assess their resiliency under appropriately stressful scenarios.
- *Liquidity requirements*. Liquidity requirements should be developed for nonbank issuers. These rules would address the types of assets eligible for the pool to "back" the stablecoin and the amount of assets vis-à-vis the outstanding amount of stablecoins.
    - The assets backing the stablecoin should represent at least 100 percent of the face value of the outstanding stablecoins before accounting for the required capital buffer. They must be safe and highly liquid. Furthermore, a material amount of the pool must provide immediate liquidity. If the pool includes "cash" or "cash equivalents," those terms need to be defined precisely and in detail. For example, the term "cash equivalents" is often understood to include treasury bills, certificates of deposit, commercial paper, and other money market instruments. Commercial paper can be illiquid and can be risky if lower rated. Likewise, the term "cash" is often ambiguous, so it should be defined precisely to include, for example, bank deposits, while excluding riskier, less liquid assets. Longer-term assets should be excluded, even if ultimate repayment is virtually certain, because they are subject to interest rate risk.
- *Reporting and auditing requirements*. Nonbank issuers should be required to report the number of stablecoins they have issued and the amount and composition of the pool of assets backing the coins. They should be required to post this information on their websites for transparency, and they should be subject to auditing by an independent certified public accountant licensed in the United States. Insured banks are already subject to independent audits.
- *Limitations on permissible activities.* Nonbank issuers should have restrictions on their commercial activities, both at the level of issuer and any affiliates, so their activities are effectively limited to those financial in nature. Banking organizations are already subject to such requirements.
- *Technological standards.* Consistent standards should apply to banks and nonbanks in terms of the types of wallets that can hold stablecoins (custodial vs. non-custodial), the blockchain protocols they use, and the technical capabilities, such as smart contracts, they enable.
- *Usage*. There should be no distinction between banks and nonbanks in terms of usage, including who may hold the stablecoin, geographic reach, or use cases (e.g., DeFi).
- *Anti-money laundering, countering the financing of terrorism, and economic sanctions obligations.* Currently, nonbank stablecoin issuers are state licensed and generally regulated as money

transmitters. As money service businesses for purposes of the BSA, they are subject to FinCEN regulation. Nonbank stablecoin issuers should also be subject to federal prudential supervision and examination to ensure compliance with AML/CFT and sanctions obligations and to avoid regulatory arbitrage.

- *Operational resilience and cybersecurity*. Nonbank issuers should be subject to federal supervision and examination for operational resilience and cybersecurity compliance.
- *Prudential requirements.* Nonbank issuers should be subject to federal examination for relevant prudential issues, such as confirmation of the composition of assets, the maintenance of necessary capital buffers, and the existence of appropriate risk management and control functions.
- *Data privacy and security.* Nonbank issuers should be subject to federal privacy regulation and data security requirements of the same type applicable to banks under the Gramm–Leach–Bliley Act and examination for compliance with those obligations.