November 3, 2022

Via Electronic Submission

United States Department of the Treasury
1500 Pennsylvania Avenue, N.W.
Washington, D.C. 20230

RE: Notice and Request for Comment – "Ensuring Responsible Development of Digital Assets"

To Whom It May Concern,

The Clearing House Association, L.L.C. ("The Clearing House")[1] appreciates efforts by the United States Department of the Treasury ("Treasury") to solicit stakeholder input on digital-asset-related illicit finance and national security risks, ways in which to support anti-money-laundering/countering-the-financing-of-terrorism ("AML/CFT") controls in the design of a potential U.S. central bank digital currency ("CBDC"), and the "Action Plan to Address Illicit Financing Risks of Digital Assets" ("Action Plan").[2] The Clearing House believes that addressing the illicit finance and national security risks of digital assets and the current digital assets ecosystem, and supporting AML/CFT controls in connection with a potential U.S. CBDC should a CBDC be determined to be in the national interest, are critical and require a number of key issues to be addressed.

In particular, The Clearing House believes that with respect to privately-issued digital assets (*e.g.*, many stablecoins) and private token-based cryptocurrency (*e.g.*, Bitcoin and Ethereum):

- A comprehensive federal prudential framework applying standards to digital assets service providers that are equivalent to those that apply to depository financial institutions when engaged in functionally similar activities is essential.
- Banks, which are subject to comprehensive regulatory and supervisory frameworks that help ensure strong customer identification/identity verification, AML/CFT screening, and sanctions compliance processes are in place, should be no less able to engage in digital-asset-related activities than nonbanks.

And that with respect to a U.S. CBDC:

- The risks associated with the possible issuance of a CBDC in the U.S. outweigh its potential benefits and, therefore, it should be determined that a CBDC is not in the national interest.

[1] 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 the core payments system infrastructure in the U.S., clearing and settling more than $2 trillion each day. *See* The Clearing House's web page at www.theclearinghouse.org.
[2] United States Department of the Treasury, "Ensuring Responsible Development of Digital Assets; Request for Comment," 87 Fed. Reg. 57,556 (Sep. 20, 2022). *See also* U.S. Department of the Treasury, "Action Plan to Address Illicit Financing Risks of Digital Assets" (link).

- If, however, the U.S. nonetheless proceeds with a CBDC, the foundational requirements in place to prevent criminal and illicit use of commercial bank money must be applied to a U.S. CBDC in such a way that criminal actors are not incentivized to use CBDC. For example, levels of identity verification and transaction monitoring should not be less for a CBDC than for commercial bank money systems.
- To the extent a U.S. CBDC is offered in an intermediated model, intermediaries must have a clear business case for assuming the customer identification/identity verification, AML/CFT screening, and sanctions compliance obligations, particularly as the risks associated with such assumption may, without fees, be unsupported by the low margins typically associated with the provision of custodial services.

I. Overview

The following overview identifies challenges and risks (A) posed by privately-issued digital assets (*e.g.*, many stablecoins) and private token-based cryptocurrency (*e.g.*, Bitcoin and Ethereum); and (B) posed by a potential U.S. CBDC. The Clearing House believes that both present unique challenges and risks.

A. The Rapid Growth of Cryptocurrency and Stablecoins, and the Risks They Present

In the past five years, the market capitalization for all cryptocurrencies increased from about $300 billion in June of 2018, to close to $3 trillion in late 2021.[3] Today, the total market capitalization appears to be just under $1 trillion.[4] Even with recent declines, the rate of growth of crypto markets is remarkable. According to the International Monetary Fund, when "the market value of crypto assets surpassed $2 trillion [in] September 2021 [it represented] a ten-fold increase [from] early 2020";[5] and according to the November 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"), 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."[6] Private estimates show a similar, if not more rapid, rate of increase – suggesting as much as a 600 percent

[3] *See* CoinMarketCap, "Global Cryptocurrency Charts[,] Total Cryptocurrency Market Cap" (estimating the total market capitalization of the cryptocurrency market at $2.9 trillion as of Nov. 9, 2021); Todd Phillips and Alexandra Thornton, "Congress Must Not Provide Statutory Carveouts for Crypto Assets," Center for American Progress (Mar. 1, 2022) (noting the collective crypto asset market capitalization peak of $2.9 trillion in Nov. 2021); *and* Speech by Acting Comptroller of the Currency Michael J. Hsu to the Institute of International Economic Law (Apr. 8, 2022) (providing market size estimates and estimating the overall size of the cryptocurrency market at "around $2 trillion").

[4] *See* "Global Cryptocurrency Charts[,] Total Cryptocurrency Market Cap," *supra* note 3 (estimating the total market capitalization of the cryptocurrency market at $943.9 billion as of Oct. 3, 2022). *See also* CoinGecko, "Cryptocurrency Prices by Market Cap" (reporting aggregate cryptocurrency market capitalization of $994 billion as of Oct. 5, 2022).

[5] Dimitris Drakopoulos, Fabio Natalucci and Evan Papageorgiou, "Crypto Boom Poses New Challenges to Financial Stability," International Monetary Fund Blog (Oct. 1, 2021).

[6] President's Working Group on Financial Markets, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, "Report on STABLECOINS" (Nov. 2021), p. 7.

increase in the stablecoin market segment from 2020 to 2021.[7] And the rate of growth is even faster when looking at specific cryptocurrency and stablecoins.[8] Just two cryptocurrencies, Bitcoin and Ethereum, represent a total market capitalization of more than $545 billion; and three stablecoins – Tether, USD Coin, and Binance USD – collectively represent more than $135.7 billion in market capitalization as of October 5.[9]

Alarmingly, this growth has occurred in an ecosystem without comprehensive and consistent supervision and examination of cryptocurrency and stablecoin issuers and arrangements. As a result, matters routinely addressed in the supervision and examination processes of regulated financial institutions – matters such as customer identification/identity verification, AML/CFT screening, and sanctions compliance – often go unaddressed, resulting in illicit and criminal use of systems and the proliferation of risks.[10] These risks are not merely theoretical. For example, misuse has presented significant AML/CFT concerns;[11] exchanges have failed to implement programs to prevent criminal misuse;[12] exchanges and arrangements appear popular for facilitation of ransom/ransomware payments;[13] exchanges and arrangements have been proven to be susceptible to hacking;[14] issuers have made material

[7] *See* Timothy G. Massad, "Regulating stablecoins isn't just about avoiding systemic risk," Brookings (Oct. 5, 2021); *and* Andrew Ross Sorkin, et al., "Here Come the Crypto Rules," The New York Times (Sep. 24, 2021) (providing estimates that equate to an approximate 600% increase from 2020 to 2021).

[8] *See, e.g.,* CoinMarketCap, "Bitcoin," at Market Cap (ALL) (showing a greater-than-2500% increase in market capitalization for Bitcoin from 2017 to 2022) (Jan. 31, 2022); CoinMarketCap, "Binance USD," at Market Cap (1Y) (showing a 1000% increase in market capitalization for Binance USD in the past year) (Jan. 31, 2022); *and* "USD Coin," at Market Cap (1Y) (showing a more-than-800% increase in market capitalization for USD Coin in the past year).

[9] As of Oct. 5, 2022. *See* CoinMarketCap.com (providing market capitalization figures for major cryptoassets).

[10] *See* Department of Justice, "High-Ranking Employee At Cryptocurrency Exchange Pleads Guilty To Bank Secrecy Act Violations," U.S. Attorney's Office Press Release (Aug. 8, 2022); Department of Justice, "Third Founder Of Cryptocurrency Exchange Pleads Guilty To Bank Secrecy Act Violations," U.S. Attorney's Office Press Release (March 9, 2022); Yvonne Lau, "Binance failed to live up to its anti-money laundering obligations, report says," Fortune (Jan. 24, 2022); *and* Leigh Cuen, "Most Crypto Exchanges Still Don't Have Clear KYC Policies: Report," CoinDesk (Sep. 13, 2021).

[11] *See* Timothy B. Lee, "Janet Yellen Will Consider Limiting the Use of Cryptocurrency," WIRED (Jan. 22, 2021) (noting that Secretary Yellen has suggested the government should "examine ways in which [it] can curtail the[ ] use [of certain digital currencies] and make sure that [money laundering] doesn't occur through those channels"); *and* Harry Robertson, "Janet Yellen says 'misuse' of cryptocurrencies like bitcoin is a growing problem, as regulators increase scrutiny after surge in interest," Business Insider (Feb. 11, 2021) (quoting Janet Yellen as saying that "misuse" of cryptocurrencies is a "growing problem").

[12] *See* "High-Ranking Employee At Cryptocurrency Exchange Pleads Guilty To Bank Secrecy Act Violations" *and* Third Founder Of Cryptocurrency Exchange Pleads Guilty To Bank Secrecy Act Violations," *supra* note 10.

[13] *See* U.S. Department of the Treasury, "Treasury Takes Robust Actions to Counter Ransomware," Press Release (Sep. 21, 2021); Department of Justice, "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside," Press Release (June 7, 2021); *and* Marsh McLennan, "Ransomware: Paying Cyber Extortion Demands in Cryptocurrency" (2022) (reporting that Bitcoin payments account for 98% of ransomware payments).

[14] Action Plan, *supra* note 2, at p. 8; David Yaffe-Bellany, "The Crypto World Is on Edge After a String of Hacks," The New York Times (Sep. 28, 2022); Ryan Browne & MacKenzie Sigalos, "Hackers have stolen $1.1 billion this year using crypto bridges. Here's why it's happening," CNBC (Aug. 10, 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); *and* Arjun Kharpal and Ryan Browne, "Hackers return

misrepresentations about key features of crypto assets and the processes that support them;[15] and crypto-asset-related services have arisen to enhance anonymity and aid the evasion of AML/CFT requirements and sanctions.[16] For these reasons, The Clearing House believes that a comprehensive federal prudential framework applying standards that are equivalent to those that apply to depository financial institutions when engaged in functionally similar activities is essential.

B. Central Bank Digital Currency

Recently, the U.S. government has shown an interest in the potential development of a U.S. CBDC. In January, the Board of Governors of the Federal Reserve System ("Fed") released its paper, "Money and Payments: The U.S. Dollar in the Age of Digital Transformation," as the "first step" in the consultative process the Fed is pursuing to explore whether a U.S. CBDC would be beneficial.[17] In March the White House issued its Executive Order on "Ensuring Responsible Development of Digital Assets," dictating policy and actions on CBDC that includes analysis of the potential implications of a U.S. CBDC on a number of areas, continued research of CBDC, and an assessment of the legislative changes necessary for the U.S. to issue a CBDC.[18] And in September several reports addressing CBDC, which were called for under the executive order, were published.[19]

---

nearly half of the $600 million they stole in one of the biggest crypto heists," CNBC (Aug. 11, 2021) (noting that $33 million of Tether was part of a successful hacking of Poly Network, a platform that connects different blockchains together). *See also* U.S. Securities and Exchange Commission, "Investor Alert: Bitcoin and Other Virtual Currency Investments" (May 7, 2014) (noting the risk that crypto currency exchanges may stop operating or permanently shut down due to fraud, technical glitches, hackers or malware).

[15] *See* "In the Matter of Investigation by Letitia James, Attorney General of the State of New York, of iFinex Inc., BFXNA Inc., BFXWW Inc., Tether Holdings Limited, Tether Operations Limited, Tether Limited, Tether International Limited," settlement agreement (Feb. 18, 2021), pp. 3-13 (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).

[16] *See, e.g.,* "Tornado Cash Privacy Solution" (details available at: link) (Tornado Cash is a "non-custodial Ethereum and ERC20 privacy solution" that "improves transaction privacy by breaking the on-chain link between the recipient and destination addresses." Tornado Cash notes that it "uses a smart contract that accepts ETH deposits that can be withdrawn by a different address"; and markets itself by stating that "[w]henever ETH is withdrawn by the new address, there is no way to link the withdrawal to the deposit, ensuring complete privacy.") *See also* U.S. Department of the Treasury, "U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats," press release (May 6, 2022); U.S. Department of the Treasury, "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash," press release (Aug. 8, 2022); Andrew Martin and Christopher Condon, "Crypto Mixer Used by North Korea Slapped with US Sanctions," Bloomberg (Aug. 8, 2022); *and* Steven Stradbrooke, "US looks to beef up Russia sanctions via crypto mixer crackdown," Coingeek (Sep. 23, 022).

[17] Board of Governors of the Federal Reserve System, "Money and Payments: The U.S. Dollar in the Age of Digital Transformation" (Jan. 14, 2022).

[18] White House, "Executive Order on Ensuring Responsible Development of Digital Assets," at "Sec. 4. Policy and Actions Related to a United States Central Bank Digital Currency" (Mar. 9, 2022).

[19] *See, e.g.,* U.S. Department of the Treasury, "The Future of Money and Payments [Report]" (Sep. 2022) (link); White House, "Policy Objectives for a U.S. Central Bank Digital Currency System" (link); *and* Office of Science and Technology Policy, "Technical Evaluation for a U.S. Central Bank Digital Currency" (link).

After careful consideration,[20] The Clearing House believes that a CBDC would pose substantial risks to the U.S. financial system – risks that cannot be adequately controlled, regardless of proposed mitigants (*e.g.*, intermediation, holding limits, etc.) – and would exacerbate illicit finance and national security risks (*e.g.*, by giving rise to cyber and operational risk) rather than solving them.[21] These risks not justified in light of the fact that every policy goal thus far articulated in support of a CBDC can be addressed through less risky, more efficient, and more economical alternatives that are either readily available in the market today, or are under development by the private sector.[22] Additionally, a U.S. CBDC is unlikely to be an effective tool for the purposes for which it has been advanced (*e.g.,* to preserve the status of the U.S. dollar as a global reserve currency and to address national security concerns). It is for these reasons that trade organizations representing every type of bank in the U.S., including small, minority, community depository institutions and credit unions, recently wrote to Congress in opposition to a CBDC, citing the lack of compelling use cases for a CBDC and the significant risks a U.S. CBDC poses.[23]

The case for a U.S. CBDC is far from compelling when one considers: (1) the long history in the U.S. of privately-issued money (and the proven ability of regulatory frameworks to address issues associated with private money);[24] (2) that the dollar is largely digital today and commercial bank money successfully serves as a low-risk settlement asset;[25] (3) that the status of the U.S. dollar as a global reserve currency has

[20] *See* The Clearing House, "On the Road to a U.S. Central Bank Digital Currency — Challenges and Opportunities" (July 2021) (link) (highlighting significant implication of certain design and implementation choices associated with a U.S. CBDC and making specific recommendations about CBDC).

[21] In particular, a CBDC would: (a) cannibalize bank deposits, as commercial bank money is converted into CBDC; (b) negatively impact lending and the cost of credit for consumers and businesses; (c) have a potentially destabilizing effect on foreign financial systems where individuals and businesses may prefer the relative safety and security of a U.S. central bank obligation to an obligation of their home central banks; (d) potentially expose the Fed to increased political pressures over time, particularly if it is in a position of making interest rate changes to CBDC or determines holding limits; and (e) is likely increase cyber and operational risk related to the money supply, but, at a minimum, concentrate risk in a way that does not occur today with paper currency. *See* Letter from Robert C. Hunter, Director of Legislative & Regulatory Affairs and Deputy General Counsel, The Clearing House, to Ann E. Misback, Secretary, Board of Governors of the Federal Reserve System, pp. 3-10 (May 20, 2022) (link)

[22] *See* Letter from Robert C. Hunter, *supra* note 21, at pp. 17-18 (providing comments to the Fed in response to its consultative paper on CBDC). *See also* Letter from Philip Keitel, Associate General Counsel & Vice President, The Clearing House, to United States Department of the Treasury, at Appendix A (Aug. 8, 2022) (link) (identifying more economical and less-risky alternatives to a U.S. that are available in the marketplace today or are under development by the private sector).

[23] Letter from the American Bankers Association, Bank Policy Institute, Consumer Bankers Association, Credit Union National Association, National Association of Federally-Insured Credit Unions, National Bankers Association, and The Clearing House to The Honorable Maxine Waters and Patrick McHenry, House Financial Services Committee (May 25, 2022) (link).

[24] *See* Bruce Champ, "Private Money in our Past, Present, and Future," Federal Reserve Bank of Cleveland (Jan. 1, 2007 (providing a historical overview of private money and money issued by specific community groups); "On the Road to a U.S. Central Bank Digital Currency — Challenges and Opportunities," *supra* note 20, at p. 7; *and* Gary B. Gorton and Jeffery Zhang, "Taming Wildcat Stablecoins" (Sep. 30, 2021).

[25] As of June 15, the Fed reported $2,527,237,000,000 Federal Reserve notes outstanding. (*See* Federal Reserve, "7. Collateral Held against Federal Reserve Notes: Federal Reserve Agents' Accounts" (as of Jun. 15, 2022).) In comparison, the total assets of commercial banks in the U.S. amounted to $22,640,528,600,000. (*See* St. Louis Fed, "Total Assets, All Commercial Banks," FRED Economic Data (as of Jun. 8, 2022).) Thus, much of what we think of today as money is commercial bank money that is digital in form.

to do with a number of factors, such as respect for the rule of law, stable government, well-regulated and efficient markets, sound U.S. economic policies, etc.,[26] not the form it takes (commercial bank money is already in digital form);[27] and (4) that payment systems in the U.S. are reliable, diverse, highly competitive, and provide consumers and businesses with an extraordinary degree of choice at low cost.[28] It is even more difficult to make a case for the development of a U.S. CBDC when one factors in the significant private and public sector efforts that are already under way to improve cross-border payments, facilitate person-to-person payments, expand operating hours (the operating hours of CHIPS and Fedwire are not presently 24x7x365, but they could be), and reduce frictions in payments – all of which will continue irrespective of U.S. or foreign CBDC. In short, there is no obvious benefit from a U.S. CBDC.

A CBDC is also likely to drastically increase cyber and operational risk relates to the money supply. CBDC exists in a digital environment with substantially greater cyber risks than exist for paper money.[29] At a minimum, CBDC, in comparison with paper money, concentrates risk.[30] In contrast to paper currency, where risks are spread out across a diverse infrastructure and the failure of any one part is unlikely to have a meaningful impact on the whole, a CBDC would offer an attractive target that could be exploited by nefarious private actors seeking to leverage CBDC for illicit activities or even hostile nations. Further, a programmable CBDC that was issued, for example with an interest payment feature, could be subject to hacking and the insertion of malicious code – something that cannot be done with paper currency.

Were a CBDC to nevertheless be introduced in the U.S., the foundational requirements in place to prevent criminal and illicit use of commercial bank money, requirements such as customer identification, customer identity verification, record-keeping, suspicious activity reporting, transaction monitoring,

---

[26] *See* Carol Bertaut, Bastian von Beschwitz & Stephanie Curcuru, "The International Role of the U.S. Dollar," FEDS Note (Oct. 6, 2021) (concluding, among other things, that while "[a] shifting payments landscape could [ ] pose a challenge to the U.S. dollar's [international] dominance … it is unlikely that technology alone [(including the introduction and growth of official digital currencies)] could alter the landscape enough to completely offset the long-standing reasons the dollar has been dominant.")

[27] *See* European Central Bank, "The international role of the euro, June 2021," at Box 8 (running model simulations on the impact of a digital euro on the international role of the euro and concluding that a digital euro "would not necessarily be a game changer for the international role of the euro, which will continue to depend to a large extent on fundamental forces, such as stable economic fundamentals, size, and deep and liquid financial markets").

[28] Congressional Research Service, "Central Bank Digital Currencies: Policy Issues," pp. 15-18 & 24-25 (Feb. 7, 2022).

[29] Such catastrophic failure recently struck the CBDC platform operated by the Eastern Caribbean Central Bank ("ECCB"), forcing the ECCB to shut down the platform leaving holders of the ECCB's CBDC in limbo. *See* "Eastern Caribbean CBDC Platform Crashes" (Feb. 1, 2022) (link).

[30] It is important to recognize that this increased cyber risk would exist both at the hub (i.e., at the Fed as operator of the CBDC system) and at the spokes (i.e., intermediaries that are holding CBDC on behalf of consumers in digital wallets). As we have seen in private cryptocurrency exchanges and wallets, the digital nature of these assets engenders significant custody and cybersecurity risks with the ability of criminal actors to abscond with staggeringly large sums of cryptocurrency with a few key strokes. (*See* Paul Vigna and Sarah E. Needleman, "Hackers Steal $540 Million in Crypto From 'Axie Infinity' Game," The Wall Street Journal (Mar. 29, 2022) (noting that since 2011 as many as 226 hacking incidents have resulted in the theft of approximately $12.1 billion in cryptocurrency, that in 2021 alone there were 75 incidents with an aggregate theft amount of $4.25 billion, and that there are no indications of increased safety in the cryptocurrency marketplace); *and* Ciphertrace/Mastercard, "Cryptocurrency Crime and Anti-Money Laundering Report" (Feb. 2021) (noting substantial fraud risk alongside thefts and hacking (observing $1.1-$2.9 billion dollar fraud schemes in 2019 and 2020, in addition to hundreds of millions of dollars in thefts and hacking)).)

AML/CFT compliance, and sanctions screening,[31] should be applied to a U.S. CBDC in such a way that criminal actors are not incentivized to use a U.S. CBDC.[32] For example, levels of identity verification and transaction monitoring should not be less for a CBDC than for commercial-bank-money-based systems. Although there may be pressure to create special rules and exceptions for a U.S. CBDC in order to balance privacy concerns,[33] these pressures should be resisted. Similar pressures to design CBDC to compete with unregulated or lightly regulated cryptocurrencies by incorporating a significant degree of anonymity, and the ability to hold and transfer value outside of the reach of creditors and AML/CFT/sanctions-compliance programs, should also be resisted. These attributes are inimical to U.S. AML/CFT policy goals, the effectiveness of U.S. sanctions programs, and the orderly administration of legal processes in the U.S. and elsewhere. In order to take full advantage of the strong customer identification/identity verification, AML/CFT screening, and sanctions compliance processes financial institutions have in place, a U.S. CBDC, to the extent that it is offered in an intermediated model, must present a clear business case for intermediaries to assume the risks associated with these obligations, which, without fees, may be unsupported by the low margins typically associated with the provision of custodial services.

II. Responses to Select Questions Posed in the RFC

With respect to specific questions posed in Treasury's RFC relating to digital-asset-related illicit finance and national security risks, support of AML/CFT controls in a potential U.S. CBDC, and the Action Plan, The Clearing House provides the following comments:

- ***Illicit Finance Risks.*** **Question 1:** Has Treasury comprehensively defined the illicit financing risks associated with digital assets?

In addition to the risks mentioned in the Action Plan, The Clearing House observes that domestic regulatory arbitrage, effects from such arbitrage, and differences in the application of the comprehensive regulatory structures to traditional financial institutions all exacerbate risks posed by digital assets.

Although the Action Plan takes into consideration the increased risks posed by jurisdictional (international) regulatory arbitrage,[34] within the U.S. different products or services offering the same functionality at the same risk level are not subject to the same regulatory framework. As a result, non-bank firms in the U.S. are able to engage in domestic regulatory arbitrage which gives them advantages over

[31] *See, e.g.,* Financial Crimes Enforcement Network, "The Bank Secrecy Act" (link).
[32] *See* "The Future of Money and Payments [Report]," *supra* note 19, at p. 5 (noting that "[a]s financial institutions have strengthened anti-money laundering controls, terrorists and other criminals have increasingly turned to cash to transfer funds – capitalizing on its anonymity, portability, and liquidity").
[33] *See Id.* at p. 26, suggesting that a U.S. "CBDC could [ ] have tiered accounts to allow for different functionality, tied to different levels of identity verification and monitoring," such that "customers without identity credentials, who are often unable to access traditional financial services, [are able] to access CBDC."
[34] Action Plan, *supra* note 2, at p. 5.

banks.[35] And as institutions (based on their type of charter or the supervisory scheme they are subject to) compete against other types of institutions, financial institutions frequently find themselves at a disadvantage against lesser- or un-regulated firms, with different regulatory frameworks applying to products and services based on the type of institution offering them and not inherent differences in vulnerability of the respective products or services. Further, when the regulation, examination, or enforcement of regulatory obligations for a certain type of financial sector considered new or emerging is delayed, this sector is allowed to accumulate profits, and therefore capitalization – at a higher speed, and at the cost of a higher risk to consumers and the marketplace – than non-sector financial firms offering similar functionality that are fully regulated. Thus, perceived increased efficiency and speed of the new financial sector is based on it being able to bypass the compliance requirements that apply to its competition.

Dangers arise not only from domestic regulatory arbitrage and an uneven domestic playing field, but from differences in the application of the comprehensive regulatory structure traditional financial institutions must operate under, particularly as BSA/AML/CFT requirements may be based on, or otherwise leverage, obligations imposed by other regulatory frameworks. For example, deceptive representations about the security of a particular platform, or the efficacy of a particular algorithm to maintain the parity of a virtual currency with a fiat currency (which may result in organizers collecting exorbitant salaries and reaping astronomical profits through initial public offerings, but cause buyers to lose all their investment) are also aspects of illicit finance covered by the BSA.[36]

- ***Illicit Finance Risks.*** **Question 2:** How might future technological innovations in digital assets present new illicit finance risks or mitigate illicit finance risks?

Any financial innovation that only takes into consideration operational efficiency, while ignoring the need to comply with the combined regulatory frameworks applicable to clearing and settlement systems, will exacerbate existing risks.[37] To avoid this, financial regulators at both the state and federal levels must

[35] *See* Financial Stability Oversight Council, "Report on Digital Asset Financial Stability Risks and Regulation" (Oct. 3, 2022), at "Executive Summary," page 5 (link), noting that "crypto-asset businesses do not have a consistent or comprehensive regulatory framework and can engage in regulatory arbitrage" and that "[s]ome crypto-asset businesses may have affiliates or subsidiaries operating under different regulatory frameworks, and no single regulator may have visibility into the risks across the entire business." While the FSOC report addresses potential financial stability risks posed by digital assets, due to incomplete regulatory coverage from regulatory frameworks other than AML/CFT, many of its insights are equally applicable to the increased systemic exposure of the financial system to illicit financial activity caused by incomplete AML/CFT regulatory coverage of digital assets providers.

[36] For example, the Anti-Money Laundering Act of 2020 amends Subchapter II of chapter 53 of title 31, ("Declaration of purpose"), in part, by adding a Section 4 that reads: "(4) assess the money laundering, terrorism finance, tax evasion, and fraud risks to financial institutions, products, or services to— (A) protect the financial system of the United States from criminal abuse; and (B) safeguard the national security of the United States…."

[37] *See* "Report on Digital Asset Financial Stability Risks and Regulation," *supra* note 35, at pp. 10-11, 2.2. Key Features of Crypto-Asset Activities, noting "[p]roponents of crypto-assets have claimed [distributed ledger technology] may have a large variety of economic, social, or security related benefits based on the technological, operational, and business model features of crypto-assets and associated activities," and that "these features also have cross-cutting implications for the financial stability risks of crypto-assets and their regulation."

clearly state (and, where appropriate, implement by regulation) the following principles that have been advanced over the past decade by regulatory interpretation: [38]

1. Financial products and services that provide the same functionality at the same level of risk will be subject to identical combined regulatory frameworks (technology agnostic); [39]
2. Financial products and services must integrate compliance functionality, including with respect to combined regulatory frameworks, before release (compliance is built in from the beginning, not added as an afterthought); and
3. New regulation must account for existing methods or technologies for providing financial products and services, and new methods or technologies for providing already-regulated financial products and services must account for existing regulation (proper deference to the economic reality of a product or service).[40]

With respect to new means of offering products and services, providers must look at the fundamental characteristics of the product or service offered to determine whether the product or service is already regulated, and not seek to use new methods/technology to seek different regulatory treatment.[41]

With respect to specific technology, the introduction of quantum computing may significantly impact the provision of financial products and services digitally. It will therefore be important that the U.S. government work closely with the intelligence and scientific communities to understand technological

[38] *See* 76 Fed. Reg. 43,585 (July 21, 2011) (modifying the definition of "money transmitter" in Bank Secrecy Act-implementing regulations to capture the transmission of any type of value that "substitutes for currency." *See also* FinCEN, FIN-2013-G001, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," Mar. 18, 2013, pp. 4-5 (applying definitions of BSA-implementing regulations to creators and sellers or convertible virtual currency).

[39] *See* "Report on Digital Asset Financial Stability Risks and Regulation," *supra* note 35, at pp. 111 - 112, Section 5.1. Consideration of Regulatory Principles, Recommendation 1, noting that some of the general principles on the applicability of current authorities, recommended by the Council to its member agencies, include: "(a) same activity, same risk, same regulatory outcome; (b) technological neutrality; [and] (c) leveraging existing authorities where appropriate." (Other general principles are directly related to the financial stability risks posed by digital asset providers.)

[40] *See* FinCEN, FIN-2019-G001, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," May 9, 2019, pp. 9-12, Section 2.1. BSA Obligations of Money Transmitters, comparing the guidance on Funds Travel Rule compliance by money transmitters operating in convertible virtual currency, with the original treatment of banks under the Funds Travel Rule (31 C.F.R. § 1010.410(f)), where banks utilizing FedWire were exempted from compliance until such time as the Federal Reserve implemented changes to its transfer format that accommodated the additional required information. *See* also "Joint Statement of Leaders of CFTC, FinCEN, SEC, on Activities Involving Digital Assets," Oct. 11, 2019.

[41] *Id.* at p. 5, Section 1.2.3. Application of BSA regulations to persons not exempt from MSB status engaged in transactions denominated in any type of value that substitutes for currency, noting that "[a] person not exempt from MSB status under 31 C.F.R. § 1010.100(ff)(8) may be a money transmitter when the person engages in transactions covered by FinCEN's definition of money transmission, regardless of the technology employed for the transmittal of value or the type of asset the person uses as value that substitutes for currency, or whether such asset is physical or virtual." *See also* "Report on Digital Asset Financial Stability Risks and Regulation," *supra* note 35, at p. 11, Section 2.2. Key Features of Crypto Asset Activities, noting that "the novel technological aspects of [distributed ledger technology] have led many crypto-asset market participants to seek different regulatory treatment for their activities while conducting similar activities to services provided by traditional institutions and posing similar risks."

developments that may quickly shift the playing field in the digital asset ecosystem and the way these developments might impact illicit finance risks.

Additionally, the private sector stands ready to accelerate digital asset innovation and to increase digital-asset activity within the regulatory perimeter, which will mitigate illicit finance risks. As one example, the Regulated Liability Network ("RLN") proposal 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).[42] Tokens exchanged over the network ("RLN tokens") would be redeemable at par value on demand, and would provide an unambiguous legal claim on the regulated issuer; and the liabilities would be fungible between regulated institutions. The RLN would enable the instant movement of value 24x7x365, and would support "programmable money" insofar as payments can be automated, made conditional on events, and integrated into other digitized processes. As another example, Partior, a shared-ledger multi-currency clearing platform, was launched as a technology company in 2021.[43] Partior is currently live with digital M1 (deposit liabilities of a commercial bank) being provided by JP Morgan (USD) and DBS (SGD) that can be transacted 24x7x365 and can utilize "smart contracts." Over time, the platform intends to cover a broad set of currencies and multiple providers for each currency.

- ***Illicit Finance Risks.*** **Question 3:** What are the illicit finance risks related to non-fungible tokens?

Non-fungible tokens may, depending on design and ultimate purpose, grant property rights to different types of assets (*e.g.*, financial or non-financial, real or virtual, denominated in fiat or virtual currency, and so on). The AML/CFT risk of non-fungible tokens largely depends on the assets they represent, their design features, and any differences between the regulation and supervision of the registration or clearance and settlement systems used to document the origination and transfer of traditional titles of ownership, and the regulation and supervision of systems used to document origination and transfer. Consistent with our response to *Illicit Finance Risks. Question 2*, it is the view of The Clearing House that there should be no regulatory or supervisory differences between traditional and emerging platforms that reflect real or virtual assets involving the same level of vulnerability to AML/CFT risk.

- ***Illicit Finance Risks.*** **Question 4:** What are the illicit finance risks related to decentralized finance (DeFi) and peer-to-peer payment technologies?

Consistent with our responses to *Illicit Finance Risks. Questions 2 and 3*, the illicit finance risks associated with either DeFi or peer-to-peer payment technologies should be viewed as the same as financial products and services that offer the same or substantially similar functionality at the same level of residual (not inherent) risk. 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 its 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 of compromised credentials being more easily accessible to bad actors, will impact any regulatory or law enforcement response.

[42] *See* Citi, "The Regulated Internet of Value" (link); *and* Tony McLaughlin, "The Regulated Internet of Value[,] Executive Summary" (link).
[43] *See* Partior, "Platform" (link).

- ***AML/CFT Regulation and Supervision.*** **Question 1:** What additional steps should the U.S. government take to more effectively deter, detect, and disrupt the misuse of digital assets and digital asset service providers by criminals?

The U.S. government should act to close the substantial gaps that exist between those AML/CFT regulations applicable to nonbank stablecoin arrangements and those applicable to Banks' payments-related activities and functionally similar stablecoin-related activity.[44] In so-doing, the government should apply the principal of same activity, same risk, same regulation. Addressing these gaps, and the AML/CFT risks related to nonbank stablecoin arrangements in general, is not only critical to strengthening and modernizing the U.S. AML/CFT regime to guard against the risks presented by stablecoins, but will also bring the U.S. more closely into alignment with the Financial Action Task Force ("FATF") Recommendations ("FATF Recommendations")[45] and Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers ("FATF Guidance"),[46] which Treasury has supported.[47]

With respect to specific actions the U.S. government can take to modernize the U.S. AML/CFT regime, more closely align with the FATF Recommendations and address the risks posed by cryptocurrency and nonbank stablecoin arrangements, The Clearing House makes the following recommendations: :

1. Apply the principal of same activity, same risk, same regulation.

2. Address disparities between customer due diligence ("CDD") requirements applicable to banks and those applicable to nonbank stablecoin arrangements;

3. Address disparities between requirements relating to correspondent relationships applicable to banks and nonbank stablecoin arrangements by utilizing FinCEN's authority under 31 U.S.C. § 5318(a)(2) or (h)(2) to issue regulations to expand the correspondent account due diligence requirements that apply to banks to apply also to virtual asset service providers ("VASPs"), including with respect to correspondent account due diligence. Specifically, The Clearing House recommends that FinCEN clarify that, for a VASP, a "correspondent relationship" covered by such regulations would include the provision of virtual currency services by one VASP to another VASP or to a foreign financial institution;

4. Address disparities between requirements relating to business relationships and transactions from higher risk countries applicable to banks and nonbank stablecoin arrangements by utilizing its

[44] *See* Letter from Robert C. Hunter, Deputy General Counsel & Director of Legislative and Regulatory Affairs, The Clearing House, to Policy Division, Financial Crimes Enforcement Network (Feb. 14, 2022) (link).
[45] FATF, "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation[,] The FATF Recommendations" (Oct. 2021) (link).
[46] FATF, "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" (Oct. 28, 2021) (link).
[47] *See* President's Working Group on Financial Markets, "President's Working Group on Financial Markets Releases Report on Recommendations on Stablecoins" Press Release (Nov. 1, 2021) (link) (noting that the U.S. will continue "leading efforts" "to encourage countries to implement international AML/CFT standards and [to] pursue additional resources to support supervision of domestic AML/CFT regulations [in order to prevent misuse of stablecoins and other digital assets]").

authority under 31 U.S.C. § 5318A(a)(1) to apply the requirements relating to enhanced due diligence ("EDD") and other special measures for jurisdictions and entities determined by FinCEN to be of primary money laundering concern that apply to banks to also apply to nonbank stablecoin arrangements (this recommendation is addressed more fully below, in our response to *Global Implementation of AML/CFT Standards.* Question 1); and

5. Address potential disparities relating to beneficial ownership identification by ensuring that VASPs, like banks, are required to identify the beneficial owners of legal entity customers and record relevant information on trusts that require the filing of a document with the secretary of state or similar office.

6. Subject money transmission service providers and VASPs to examination for BSA/AML/CFT and banks and bank holding companies are.

7. Mandate that digital asset intermediaries, trading platforms, accounting platforms (*e.g.*, ledgers), and any other kind of digital asset service provider that operates with customers located in the U.S., incorporates in the U.S. under an existing legal-entity type.

8. Mandate that customers of federally regulated financial institutions be either natural or legal persons.

9. Coordinate with state, local, and tribal authorities to ensure that digital asset service providers are covered under the same regulatory frameworks as govern service providers for similar products denominated in fiat currency or transacted via traditional platforms (applying the same activity, same risk, same regulation principal).

Some of these recommendations are described in greater detail below, as well as in our response to *Global Implementation of AML/CFT Standards. Question 1*, and are, we believe, consistent with several of the policy goals articulated in Priority Actions 2, 4, and 6 of the Action Plan.

Additionally, to the extent that the Financial Crimes Enforcement Network ("FinCEN") implements the CTA and the Anti-Money Laundering Act of 2020 (the "AML Act") in the future, The Clearing House encourages FinCEN to do so in a manner that minimizes unnecessary burdens on banks and ensures consistent and harmonious reporting of beneficial ownership information. In doing so, The Clearing House urges FinCEN to balance data accuracy, reliability, and utility with compliance burdens.

Customer Due Diligence. Banks and other financial institutions (that are not money services businesses ("MSBs")) must have a customer identification program ("CIP") to collect information from a customer (*i.e.*, name, date of birth, address and identification number) and verify the identity of a customer using documentary or non-documentary methods prior to opening an account for such customer.[48] MSBs, however, are not subject to detailed identity verification and CDD requirements as a general matter. FinCEN regulations require MSBs to have policies and procedures to verify customer identification,[49] but as a general matter only MSBs that are providers or sellers of prepaid access are subject to express obligations

[48] 31 C.F.R. § 1020.220.
[49] 31 C.F.R. § 1022.210(d)(1)(i)(A).

to have policies and procedures to collect information about a person with which they engage.[50] Overall, given that nonbank stablecoin issuance is more closely aligned to deposit-like activity, the CIP and CDD rules should apply directly to VASPs.

The FATF Guidance provides that VASPs should collect relevant CDD information when they provide services to or engage in covered virtual asset activities for on or behalf of customers.[51] The FATF Recommendations provide additional detail relevant to this guidance. Specifically, the FATF Recommendations state that financial institutions should be required by law or other enforceable means to undertake CDD measures when: (i) establishing business relations; (ii) carrying out occasional transactions: (a) above the applicable designated threshold ($1,000 for VASPs specifically), or (b) that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16; (iii) there is a suspicion of money laundering or terrorist financing; or (iv) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.[52] While FATF gives countries latitude to determine how they impose specific CDD obligations, in general CDD measures applied using a risk-based approach should include: (i) identifying the customer and verifying the customer's identity using reliable source documents, data, or information; (ii) identifying the beneficial owner of legal entity customers such that the financial institution is satisfied that it knows who the beneficial owner is; (iii) understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; (iv) conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business, and risk profile, including, where necessary, the source of the funds.[53]

To address the risks associated with nonbank stablecoin arrangements, and disparities between CDD requirements applicable to non-bank stablecoin arrangements and those applicable to banks' payments-related activities and, generally, to banks engaged in functionally similar stablecoin activities, The Clearing House recommends that FinCEN, possibly in connection with supporting actions notes in Priority Action 4 of the Action Plan, utilize its authority under 31 U.S.C. §§ 5318(a)(2) and (h)(2) to:

- Lower the $3,000 threshold to $1,000 for transactions for which VASPs are required to verify the identity of customers that are not established customers;
- Adopt a CIP-style requirement for VASPs before carrying out transactions for all persons (not just non-established customers for transmittals of funds in the amount of $3,000 or more or for transactions in currency of more than $10,000); and

[50] 31 C.F.R. § 1022.210(d)(1)(iv).
[51] "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers," *supra* note 46, at pp. 78-81. The recommendation flows from recognition that there has been a large increase in the use of VA's to collect ransomware payments and to commit and launder the proceeds of fraud, and that the pace, sophistication and costs of ransomware attacks is likely to grow. (*Id.* at p. 12.) FATF goes on to note that "VAs are a vital tool for ransomware actors, without which their underlying crime would be much harder to monetize" and that "illicit actors are taking advantage of poor CDD screening processes within VASPS for ML/TF purposes, which underscores the importance of effective, on-the-ground implementation[.]" (*Id.*)
[52] *Id.* at pp. 49 & 79-81.
[53] *Id.* at pp. 37, 48-50, 52-54, 66, 69-70, 73 & 79-81.

- Conduct ongoing diligence if there is a suspicion of money laundering or terrorist financing, or the VASP has doubts about the veracity or adequacy of previously obtained customer identification data.

VASPs & Correspondent Relationships. The FATF Guidance anticipates that VASPs will comply with requirements regarding the management of correspondent relationships and defines "correspondent relationship" for VASPs as the provision of VASP services by one VASP to another VASP or a financial institution.[54] The FATF Recommendations provide that financial institutions should be required, in relation to correspondent relationships, to: (i) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision; (ii) assess the respondent institution's AML/CFT controls; (iii) obtain approval from senior management before establishing new correspondent relationships; (iv) clearly understand the respective responsibilities of each institution; and (v) with respect to "payable-through accounts," be satisfied that the respondent bank has conducted CDD on the customers having direct access to accounts of the correspondent bank, and be able to provide relevant CDD information upon request to the correspondent bank.

The Bank Secrecy Act ("BSA") requires that each financial institution that establishes, maintains, administers, or manages a correspondent account in the U.S. for a non-U.S. person must establish appropriate, specific, and, where necessary, enhanced, due diligence policies, procedures, and controls that are reasonably designed to detect and report instances of money laundering through those accounts.[55] The Bank Secrecy Act also requires additional standards for correspondent accounts for higher-risk foreign banks.[56]

The Bank Secrecy Act defines a "correspondent account" as "an account established to receive deposits from, make payments on behalf of a foreign financial institution, or handle other financial transactions related to such institution."[57] An "account": (i) means a formal banking or business relationship established to provide regular services, dealings, and other financial transactions; and (ii) includes a demand deposit, savings deposit, or other transaction or asset account and a credit account or other extension of credit.[58]

FinCEN has promulgated regulations applying the correspondent account requirements of the Bank Secrecy Act to some types of financial institutions, such as banks, but not MSBs and, therefore, not VASPs. For example, by regulation, banks are subject to enhanced CDD requirements for correspondent accounts that they provide to foreign financial institutions. The bank CDD program must include:

---

[54] "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers," *supra* note 46, pp. 52-54.
[55] 31 U.S.C. § 5318(i)(1).
[56] 31 U.S.C. § 5318(i)(2).
[57] 31 U.S.C. § 5318A(e)(1)(B).
[58] 31 U.S.C. § 5318A(e)(1)(A). FinCEN has the authority to define by regulation, with respect to an MSB, the term "account" and to include within the meaning of the term any arrangements similar to correspondent accounts and payable-through accounts. (31 U.S.C. § 5318A(e)(2).)

- Assessing the money laundering risk presented by such a correspondent account, based on a consideration of all relevant factors;
- Applying risk-based procedures and controls to each such correspondent account reasonably designed to detect and report known or suspected money laundering activity, including a periodic review of the correspondent account activity sufficient to determine consistency with information obtained about the type, purpose, and anticipated activity of the account; and
- Determining whether the correspondent account is maintained for a foreign bank that operates under certain enumerated authorities (*e.g.*, offshore banks). Such accounts will be subject to additional due diligence requirements, such as obtaining identification information of authorized users of payable-through accounts, source of funds, and beneficial ownership.[59]

The Bank Secrecy Act requires that a limited set of financial institutions, excluding MSBs, and therefore VASPs, but including banks, are: (i) prohibited from establishing, maintaining, administering, or managing a correspondent account in the U.S. for, or on behalf of, a foreign shell bank; and (ii) required to take reasonable steps to ensure that any correspondent account established, maintained, administered, or managed in the U.S. for a foreign bank is not being used by that foreign bank to indirectly provide banking services to a foreign shell bank.[60] FinCEN has implemented these statutory requirements for banks and other financial institutions enumerated in the Bank Secrecy Act but has not applied them to MSBs or VASPs.[61]

To address the risks associated with nonbank stablecoin arrangements, The Clearing House recommends that FinCEN utilize its authority under 31 U.S.C. § 5318(a)(2) or (h)(2) to issue regulations to expand the correspondent account due diligence requirements that apply to banks to apply also to VASPs, including with respect to payable-through account due diligence. Specifically, the Clearing House recommends that FinCEN clarify that, for a VASP, a "correspondent relationship" covered by such regulations would include the provision of virtual currency services by one VASP to another VASP or to a foreign financial institution. This recommendation is broadly consistent with policy goals articulated in Priority Actions 2, 4, and 6 of the Action Plan.

Transparency & Beneficial Ownership. FATF Guidance provides that VASPs should comply with FATF Recommendations regarding beneficial ownership.[62] FATF Recommendations provide that countries should take measures to prevent the misuse of legal entities for money laundering or terrorist financing, including ensuring that there is adequate, accurate, and timely information on the beneficial ownership and control of legal persons and accurate and timely information on express trusts that can be obtained or accessed in a timely fashion by relevant authorities.

[59] 31 C.F.R. § 1010.610.
[60] 31 U.S.C. §§ 5318(j)(1), (2).
[61] *See* 31 C.F.R. §§ 1010.630(a)(1)(i) & 1010.630(a)(1)(ii).
[62] "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers," *supra* note 46, at pp. 51-52, 63, 67-68, 80 & 85.

In January 2021, Congress passed the Corporate Transparency Act, which will require certain entities to file reports with FinCEN identifying and providing information on their beneficial owners.[63] FinCEN has issued a final rule to implement the reporting requirements.[64]

To address the risks associated with nonbank stablecoin arrangements, The Clearing House recommends that FinCEN engage in additional rulemaking to extend its final rule to ensure that VASPs, like banks, are required to identify the beneficial owners of legal entity customers and record relevant information on trusts that require the filing of a document with the secretary of state or similar office.

Legal Personality Requirement. While some regulatory frameworks (such as the BSA) apply to natural persons, legal persons, *and* unincorporated entities, more optimal regulatory and law enforcement outcomes will result from products and services providers – specifically, digital asset intermediaries, trading platforms, accounting platforms (ledgers), and any other kind of digital asset service provider that operates with customers located in the U.S. – being required to incorporate in the U.S. under a given subset of the existing types of legal entity.[65] Requiring providers to have a clear legal personality would also help clarify the contractual remedies available to providers' customers.[66]

- ***AML/CFT Regulation and Supervision.*** **Question 2:** Are there specific areas related to AML/CFT and sanctions obligations with respect to digital assets that require additional clarity?

Consistent with our responses to *Illicit Finance Risks. Questions 1 through 3*, additional clarity would benefit the obligations of market participants as well as the protections available from the federal government to regulated entities that comply with voluntary obligations. For example, the Action Plan mentions that Section 314B of the USA PATRIOT Act permits financial institutions to, upon providing notice to the Treasury Department, share information with one another to identify and report to the federal government activities that may involve money laundering or terrorist activity. There is not, however, a clear safe-haven from the consequences[67] of a good faith exchange of information that ultimately does not involve money laundering or terrorist activity but nevertheless results in the subject losing access to financial services.

[63] The Corporate Transparency Act of 2021 was passed by Congress as part of the Anti-Money Laundering Act of 2020. Both were contained within the National Defense Authorization Act for Fiscal Year 2021. Additional information on the Anti-Money Laundering Act of 2020 is available here (link).

[64] 87 Fed. Reg. 59,498 (Sep. 30, 2022). While the definition of "reporting companies" in the final rule covers a large number of entities, it does not specially address VASPS. Additionally, exceptions, such as the exception for money transmitting businesses, may function to exempt VASPs from requirements to identify the beneficial owners of legal entity customers and to record certain information.

[65] For purposes of this comment, a legal entity is as 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.

[66] *See* "Report on Digital Asset Financial Stability Risks and Regulation," *supra* note 35, at p. 116, Section 5.3.2. Regulatory Arbitrage. Recommendation 4, noting that "[t]here may 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."

[67] For example, an institution that shares information could potentially be liable to an impacted consumer under the Fair Credit Reporting Act.

- ***AML/CFT Regulation and Supervision.*** **Question 3:** What existing regulatory obligations in your view are not or no longer fit for purpose as it relates to digital assets? If you believe some are not fit for purpose, what alternative obligations should be imposed to effectively address illicit finance risks related to digital assets and vulnerabilities?

Expansion of Regulatory Premise. Current BSA-implementing regulations rely at times on the intervention of financial intermediaries that will obtain, verify, retain, and report information to the appropriate regulators about the parties to a given transaction. Even when defining financial agencies, the statute states that such definition will only apply to those persons that perform services in furtherance of, or that are similar to, those provided by financial intermediaries. However, as mentioned by the Action Plan, digital assets do not require third-party intermediaries. It is possible that, for BSA purposes, transactions in digital assets may resemble peer-to-peer transfers of monetary instruments, but with a much higher velocity and cross-border scope. The BSA must deal with the need to apply regulatory requirements to non-financial intermediaries ("users," as defined in FinCEN's 2013 Guidance), in a way that ensures viable procedures for examination and enforcement of such requirements.

MSB Obligations. Key BSA obligations of most types of MSBs are less well defined than those applicable to federally regulated financial institutions. To mitigate domestic regulatory arbitrage and ensure a level playing field, regulation and oversight must be based on the inherent risk of the financial product/service and institution offering the product/service.

Funds Recordkeeping and Travel Rule Obligations. VASPs should be required to comply with the same funds transfer recordkeeping and travel rule obligations that apply to banks and traditional money transmitters.[68] Compliance includes applying the Funds Recordkeeping rule to transactions between hosted and unhosted wallets, and applying the Funds Travel Rule to transactions between wallets hosted at VASPs. VASPs must be examined for compliance with both regulations, and subject to enforcement actions, where appropriate.[69]

- ***AML/CFT Regulation and Supervision.*** **Question 4:** What regulatory changes would help better mitigate illicit financing risks association with digital assets?

In relation to our responses to *Illicit Finance Risks. Questions 1 through 3*, The Clearing House notes that, since 2013, some key regulatory responses to the illicit financing risks of digital assets have been issued in the form of regulatory interpretation.[70] As a result, these administrative agency actions are more

[68] *See* FFIEC, "Funds Transfers Recordkeeping—Overview" (link) *and* FinCEN "Funds ' Travel' Regulations: Questions & Answers" (link).
[69] *See* "Report on Digital Asset Financial Stability Risks and Regulation," *supra* note 35, p 112, Section 5.2. Continued Enforcement. Recommendation 2, noting that "[t]he Council recommends that agencies continue to enforce existing rules and regulations, including but not limited to product, exchange, and other applicable market participant registration requirements…."
[70] *See, e.g.,* FinCEN, FIN-2013-G001, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies" (Mar. 18, 2013); *and* FinCEN, FIN-2019-G001, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies" (May 9, 2019).

susceptible to challenge.[71] Final rules instead issued the through notice and comment process, pursuant to the Administrative Procedure Act, would provide additional clarity and legal certainty to the marketplace.

- ***AML/CFT Regulation and Supervision.*** **Question 5:** How can the U.S. government improve state-state and state-federal coordination for AML/CFT regulation and supervision for digital assets?

The Clearing House recommends regulators explore development of standardized push-notification systems (*e.g.*, AirDrop) for the delivery of important supervisory notices to digital platforms (*e.g.*, digital wallets), and establish rules for non-enablement of required, updated delivery methods of supervisory notices.

- ***AML/CFT Regulation and Supervision.*** **Question 7:** What additional steps should the U.S. government consider to address the illicit finance risks related to mixers and other anonymity-enhancing technologies?

With respect to mixers, and operators of anonymity-enhancing technologies, the U.S. government should continue its efforts to hold mixers liable for BSA/AML violations. While there may be legal uncertainty in this space, ensuring compliance with existing laws, or updating those laws should they be found not to apply by a court, is critical to preventing illicit activities involving digital assets. Thus, third-party providers of anonymizing services that fall under the BSA definition of "money transmitter," should be subjected to the full BSA regulatory framework, including registration with FinCEN, and VASPs issuing or dealing in anonymity-enhanced digital/virtual currencies should also subject to the BSA as "money transmitters." In addition, the U.S. government should consider subjecting digital ledgers to reporting requirements similar to those applicable to credit card networks[72] to the extent that they are engaged in a substantially similar function. 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.

- ***AML/CFT Regulation and Supervision.*** **Question 8:** What steps should the U.S. government take to effectively mitigate the illicit finance risks related to DeFi?

See supra our responses to *Illicit Finance Risks. Questions 1 through 3* and *AML/CFT Regulation and Supervision. Questions 1.*

- ***Global Implementation of AML/CFT Standards.*** **Question 1:** How can Treasury most effectively support consistent implementation of global AML/CFT standards across jurisdictions for digital assets, including virtual assets and VASPs?

The first step in effectively supporting consistent implementation of global AML/CFT standards across jurisdictions should be to ensure that U.S. requirements are consistent with such standards. Treasury can support consistent implementation of standards by addressing disparities between requirements

[71] *See "*Interagency Statement Clarifying the Role of Supervisory Guidance," Sep. 11, 2018.
[72] *See, e.g.,* FinCEN, "Anti-Money Laundering Programs for Operators of a Credit Card System," 67 Fed. Reg. 21,121 (Apr. 29, 2002).

relating to business relationships and transactions from higher risk countries applicable to banks and nonbank stablecoin arrangements. This can be done by Treasury utilizing its authority under 31 U.S.C. § 5318A(a)(1) to apply the requirements relating to enhanced due diligence ("EDD") and other special measures for jurisdictions and entities determined by FinCEN to be of primary money laundering concern that apply to banks to also apply to nonbank stablecoin arrangements.

FATF Guidance provides that VASPs should apply EDD measures to business relationships and transactions from higher risk countries.[73] FATF Recommendations provide that financial institutions should be required to apply EDD measures to business relationships and transaction with natural and legal entities and financial institutions from countries for which this is called for by FATF.[74] The type of EDD measures applied should be effective and proportionate to the risks.[75]

Banks and other types of financial institutions (but not MSBs, and therefore not VASPs) are required to implement special measures for jurisdictions and entities determined by FinCEN to be of primary money laundering concern.[76] MSBs (including VASPs) are not explicitly subject to the special measures against higher-risk countries and foreign entities as required by the FATF Recommendations and Guidance.[77]

- ***Private Sector Engagement and AML/CFT Solutions.*** **Question 1:** How can Treasury maximize public-private and private-private information sharing on illicit finance and digital assets?

There are several actions the U.S. government (including the Treasury Department) can take to maximize information. The sharing of confidential supervisory information between federal prudential regulators and market regulators, for example, would, with appropriate safeguards in place, help facilitate timely transfer of key information (e.g., a report on AML/CFT risks of specific entities could be shared by one regulators with another) and would create efficiencies for regulators and regulated entities. As an additional example, the government could work with private entities to establish a system for scoring the robustness of identification systems utilized by providers or platforms. Such a system would allow regulators to focus oversight on entities utilizing less-robust customer-identification/KYC processes, and could eventually prevent criminal actors from gaining access to systems.

The Clearing House also encourages the Treasury Department to closely scrutinize any improvement claims from providers of new technologies, and to carefully determine whether any contractual, regulatory, or internal controls are being short-changed to obtain claimed or seeming

[73] "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers," *supra* note 46, at p. 66, Recommendation 19.
[74] *Id.*
[75] *Id.* at pp. 40 & 43.
[76] 31 C.F.R. §§ 1010.651-661.
[77] FinCEN guidance does suggest, however, that certain due diligence requirements regarding foreign agents or foreign counterparties may apply to certain hosted wallet providers for convertible virtual currencies. (*See* FinCEN, FIN-2019-G001, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," at p. 16, note 54.)

improvements.[78] Often, net improvements in cost, service availability, and transaction speed, as well as market efficiencies, are only realized when the provider also complies with the full, combined regulatory framework structure that applies to its competition. The Treasury Department should recognize that while some efficiency issues of traditional financial intermediaries are due to their continuing use of legacy systems, traditional financial intermediaries have introduced redundancy and cross-checking procedures that protect consumers, the intermediary, and the financial system from repeat and unforeseen crises. New and emerging technologies may not prove resilient in a crisis and may contribute materially to a crisis. Thus, any statements that tail events "cannot happen here" should be closely examined.

- ***Private Sector Engagement and AML/CFT Solutions.*** **Question 2:** How can Treasury, in concert with other government agencies, improve guidance and public-private communication on AML/CFT and sanctions obligations with regard to digital assets?

  While very useful, fraud and other illicit finance typologies tend to describe behaviors that are necessary, but not sufficient, to categorize an activity as suspicious. For example, the same typologies mentioned in the context of money laundering may apply to the traditional business model of certain sectors, such as trading companies. Financial intermediaries would benefit from better information about the differences between the utilization of a given typology by criminals, and their utilization by lawful industry sectors, to mitigate the costly effect of an excessive number of false positives.

- ***Private Sector Engagement and AML/CFT Solutions.*** **Question 5:** Are there additional steps the U.S. government can take to promote the development and implementation of innovative technologies designed to improve AML/CFT compliance with respect to digital assets?

  One of the most valuable contributions, if not the most valuable contribution, the U.S. government could make to the innovation of both traditional and digital asset financial transactions would be to develop and sponsor a digital identity protocol that serves as a means of identifying a natural or legal subject while satisfying both the operational requirements of financial intermediaries and the needs of law enforcement.

- ***Private Sector Engagement and AML/CFT Solutions.*** **Question 6:** How can law enforcement and supervisory efforts related to countering illicit finance in digital assets better integrate private sector resources?

[78] *See* "Report on Digital Asset Financial Stability Risks and Regulation," *supra* note 35, pp. 10 & 12, Section 2.2. Key Features of Crypto-Asset Activities, Background and Pseudonymity, noting that "[p]roponents of crypto-assets have claimed [distributed ledger technology] may have a large variety of economic, social, or security related benefits based on the technological, operational, and business model features of crypto-assets and associated activities," that "some market participants attempt to use pseudonymity to evade compliance with legal and regulatory obligations," *and* "the purported benefits of pseudonymity may be largely illusory for consumers and investors who access crypto assets through intermediaries that verify their identities."

Most supervisory reporting information (such as bank call reports), while containing vast amounts of detailed data, is designed to satisfy safety and soundness requirements and may therefore not be equally suitable for developing a picture of the size and composition of financial products, services, and markets for purposes of BSA/AML/CFT risk determination. It would be advantageous to all parties to start public/private discussions on how to supplement these existing reports with transactional and customer segment data that would let both regulators and regulated entities develop better systemic description of their common ecosystem.[79] Further, while there is significant amount of data coming from many different sources, information coming from one source may be combined with the information coming from another, requiring vast amounts of resources to conduct meaningful analyses, extracting, and transform this data. Were the U.S. government, or a multi-national body, to, in consultation with the private sector, propose a set of working definitions, formats, and standard content, then it would be possible to develop a data mart that could provide public and private sector analysts with actionable standardized data at a fraction of current costs. Any attempts by the private sector to achieve similar results are likely to fail or take a long time.

- ***Central Bank Digital Currency.*** **Question 1:** How can Treasury most effectively support the incorporation of AML/CFT controls into a potential U.S. CBDC design?

The risks associated with the possible issuance of a CBDC in the U.S. outweigh its potential benefits and, therefore, it should be determined that a CBDC is not in the national interest. However, if a CBDC was to be issued in the U.S., the foundational requirements in place to prevent criminal and illicit use of commercial bank money, requirements such as customer identification, customer identity verification, record-keeping, suspicious activity reporting, transaction monitoring, AML/CFT compliance, and sanctions screening,[80] should be applied to a U.S. CBDC in such a way that criminal actors are not incentivized to use a U.S. CBDC.[81] For example, levels of identity verification and transaction monitoring should not be less for a CBDC than for commercial-bank-money-based systems. Although there may be pressure to create special rules and exceptions for a U.S. CBDC in order to balance privacy concerns,[82] these pressures should be resisted. Similar pressures to design CBDC to compete with unregulated or lightly regulated cryptocurrencies by incorporating a significant degree of anonymity, and the ability to hold and transfer value outside of the reach of creditors and AML/CFT/sanctions-compliance programs, should also be resisted. These attributes are inimical to U.S. AML/CFT policy goals, the

[79] *See* "Report on Digital Asset Financial Stability Risks and Regulation," *supra* note 35, p. 119, Section 5.4. Ensuring Regulation is Informed by Appropriate Data. Recommendation 9, noting that "[t]he Council recommends a coordinated government-wide approach to data and to the analysis, monitoring, supervision, and regulation of crypto-asset activities," and that "member agencies consider the use of available data collection powers in order to facilitate assessments of the financial risks related to crypto assets, as part of data sharing and coordination among the members."

[80] *See, e.g.,* Financial Crimes Enforcement Network, "The Bank Secrecy Act" (link).

[81] *See* "The Future of Money and Payments [Report]," *supra* note 19 , p. 5 (noting that "[a]s financial institutions have strengthened anti-money laundering controls, terrorists and other criminals have increasingly turned to cash to transfer funds – capitalizing on its anonymity, portability, and liquidity").

[82] *See Id.* at p. 26, suggesting that a U.S. "CBDC could [ ] have tiered accounts to allow for different functionality, tied to different levels of identity verification and monitoring," such that "customers without identity credentials, who are often unable to access traditional financial services, [are able] to access CBDC."

effectiveness of U.S. sanctions programs, and the orderly administration of legal processes in the U.S. and elsewhere. Additionally, were a U.S. CBDC to be programmable, the programmable feature should be leveraged to ensure that U.S. CBDC cannot be bought or sold by someone who has not been vetted for AML/CFT by a suitable intermediary, such as a as a regulated financial institution.

III. Conclusion

Privately-issued digital assets, and private token-based cryptocurrency, have grown tremendously over the past decade. Today, these digital assets have neared, or possibly even surpassed, $1 trillion in market capitalization. Given the rapid growth of these assets, and the significant challenges and risks they represent, the work Treasury is doing to solicit stakeholder input on digital-asset-related illicit finance and national security risks, ways in which to support AML/CFT controls in the design of a potential U.S. CBDC, and the Action Plan is critical. The Clearing House believes that to safeguard against the risks posed by privately-issued digital assets, a comprehensive federal prudential framework applying standards to digital assets service providers that are equivalent to those that apply to depository financial institutions when engaged in functionally similar activities is essential. The Clearing House further believes that Banks, which are subject to comprehensive regulatory and supervisory frameworks that help ensure strong customer identification/identity verification, AML/CFT screening, and sanctions compliance processes are in place, should be no less able to engage in digital-asset-related activities than nonbanks.

With respect to a potential U.S. CBDC, The Clearing House believes that the risks associated with the possible issuance of a CBDC in the U.S. outweigh its potential benefits, particularly in light of the ability of existing alternatives to achieve the policy goals that have been advanced in support of CBDC. If, however, the U.S. nonetheless proceeds with a CBDC, The Clearing House believes the foundational requirements in place to prevent criminal and illicit use of commercial bank money should be applied to a U.S. CBDC in such a way that criminal actors are not incentivized to use CBDC. Additionally, to the extent a U.S. CBDC is offered in an intermediated model, intermediaries must have a clear business case for assuming the customer identification/identity verification, AML/CFT screening, and sanctions compliance obligations associated with an intermediated U.S. CBDC.

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 me using the contact information provided below.

Yours very truly,

/S/

Philip Keitel
Associate General Counsel & Vice President
(646) 709-3026
Philip.Keitel@TheClearingHouse.org