

February 14, 2022

Submitted to: www.regulations.gov

Policy Division
Financial Crimes Enforcement Network
P.O. Box 39
Vienna, VA 22183

Re: *Review of Bank Secrecy Act Regulations and Guidance* –
Docket Number FINCEN-2021-0008

Dear Sir or Madam:

The Clearing House Association, L.L.C. (“The Clearing House”)¹ appreciates this opportunity to comment on the request for information and comment (“RFI”) issued by the Financial Crimes Enforcement Network (“FinCEN”), soliciting comment on ways to streamline, modernize, and update the anti-money laundering and countering the financing of terrorist (“AML/CFT”) regime in the United States.² The payments system in the U.S. is rapidly evolving and it is important that the AML/CFT regime remain current with recent developments in order to accomplish the overarching goal of protecting the financial system from threats to national security posed by various forms of financial crime, including money laundering, the financing of terrorism, and proliferation.

One of the most significant developments that has occurred since FinCEN last undertook a review of the U.S. AML/CFT regime is the rapid growth of stablecoins. Both banks and non-banks are today engaged in stablecoin issuance, transfer, conversion, and other functions. Stablecoins can present substantial risks related to potential money laundering, terrorist financing, and proliferation. These risks are well-managed within the highly regulated and supervised bank environment. Substantial gaps exist, however, between those AML/CFT regulations applicable to nonbank stablecoin arrangements and those applicable to Banks’ payments-related activities and functionally similar stablecoin-related activity. As is more fully set forth below, The Clearing House urges FinCEN to address AML/CFT risks related to nonbank stablecoin arrangements, and to specifically address the gaps in regulation that exist between nonbank stablecoin arrangements and banks’ payments-related activities and

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 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 “Review of Bank Secrecy Act Regulations and Guidance,” 86 Fed. Reg. 71,201 (December 15, 2021).

functionally similar stablecoin-related activity.³ The Clearing House commends FinCEN for its willingness to improve and strengthen the AML/CFT regime of the U.S. and notes that modernizing and updating the U.S. AML/CFT regime would be incomplete without addressing the many AML/CFT risks from nonbank stablecoin arrangements.

I. *Executive Summary*

The U.S. has seen remarkable growth in the use and value of stablecoins over the past year, growth which promises to continue, if not accelerate, in the future. Although many stablecoins are currently used to facilitate trading, lending, or borrowing of other digital assets, proponents believe that stablecoins could become widely used as a means of payment and have the potential to scale rapidly. Stablecoins present a host of AML/CFT risks, including their potential growth and reach, the degree to which stablecoin arrangements permit anonymity, the usability of stablecoins, the exchangeability of stablecoins for fiat currency, and the lack of comprehensive regulation of nonbank stablecoin issuers and nonbank stablecoin arrangements.

There are currently meaningful gaps between how AML/CFT regulations apply to banks' payments-related activities and functionally similar stablecoin-related activity and how such regulations apply to nonbank stablecoin arrangements. To address the risks associated with nonbank stablecoin arrangements, FinCEN should address those gaps. Doing so is not only critical to strengthening and modernizing the U.S. AML/CFT regime to guard against the risks presented by stablecoins, but it will also bring the U.S. more closely into alignment with the Financial Action Task Force ("FATF") Recommendations ("FATF Recommendations")⁴ and Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers ("FATF Guidance"),⁵ which the U.S. Treasury has supported.⁶

To modernize the U.S. AML/CFT regime and address the risks posed by nonbank stablecoin arrangement, The Clearing House recommends that FinCEN:

³ The Clearing House understands that other trade associations may be proposing changes to the AML/CFT regime for banks. To the extent FinCEN were to make such changes, The Clearing House assumes that FinCEN would examine whether to make corresponding changes to the AML/CFT regime for nonbank stablecoin arrangements.

⁴ FATF, "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation[,] The FATF Recommendations" (Oct. 2021) (available at: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>).

⁵ FATF, "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" (Oct. 28, 2021) (available at: <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html>).

⁶ 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) (available at: <https://home.treasury.gov/news/press-releases/jy0454>) (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]").

1. Address disparities between customer due diligence (“CDD”) requirements applicable to banks and those applicable to nonbank stablecoin arrangements by using FinCEN’s 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 Virtual Asset Service Providers (“VASPs”)⁷ are required to verify the identity of customers that are not established customers;
- Adopt a customer-identification-program-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);
- Require VASPs to conduct ongoing diligence if there is a suspicion of money laundering or terrorist financing or if the VASP has doubts about the veracity or adequacy of previously obtained customer identification data; and
- Require VASPs to verify the identity of beneficial owners of legal entity customers.

2. 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 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.

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

4. Address potential disparities relating to beneficial ownership by proceeding with FinCEN’s rulemaking to implement reporting requirements regarding beneficial owners and ensure that VASPs, like banks, are required to identify the beneficial owners of legal entity

⁷ The term “Virtual Asset Service Provider” is defined by FATF as “any natural or legal person who is not covered elsewhere under [FATF] Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: (i) exchange between virtual assets and fiat currencies; (ii) exchange between one or more forms of virtual assets; (iii) transfer of virtual assets; (iv) safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and (v) participation in a provision of financial services related to an issuer’s offer and/or sale of a virtual asset.” (“International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation[,] The FATF Recommendations,” *supra* note 4, at. p. 130.)

customers and record relevant information on trusts that require the filing of a document with the secretary of state or similar office.

II. Discussion

A. The Growth of Stablecoins

Stablecoins are growing at a remarkable pace, particularly nonbank stablecoin arrangements. According to the Report on Stablecoins issued by the President’s Working Group on Financial Markets, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, 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.”⁸ And according to research conducted in connection with a House Financial Services Committee hearing on stablecoins held earlier this month, “[a]s of February 3, 2022, stablecoins reached an estimated \$174 billion in market capitalization.”⁹ Private estimates show a similar, if not more rapid, rate of increase (*e.g.*, a ~600 percent increase).¹⁰ As of the end of last month (January 2022), the top three stablecoins by market cap are:¹¹

- Tether (USDT – issued by Tether Limited) \$78.2 billion;
- USD Coin (USDC – issued by Circle) \$49.8 billion; and
- Binance USD (BUSD – issued by Binance) \$15.3 billion.

Although many stablecoins are used in the U.S. today to facilitate trading, lending, or borrowing of other digital assets, predominantly on or through digital asset trading platforms, proponents believe stablecoins could become widely used by households and businesses as a

⁸ 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) (“PWG Report”), p. 7 (available at: https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf).

⁹ Majority Committee Memorandum, “Digital Assets and the Future of Finance: The President’s Working Group on Financial Markets’ Report on Stablecoins” (Feb. 3, 2022), p. 2 (available at: <https://financialservices.house.gov/uploadedfiles/hhrg-117-ba00-20220208-sd002.pdf>). Information on the full hearing is available at: <https://financialservices.house.gov/events/eventsingle.aspx?EventID=409026>. See also Senate Banking Committee, “Stablecoins: How Do They Work, How Are They Used, and What Are Their Risks?” Full Committee Hearing (Dec. 14, 2021) (available at: <https://www.banking.senate.gov/hearings/stablecoins-how-do-they-work-how-are-they-used-and-what-are-their-risks>).

¹⁰ See Timothy G. Massad, “Regulating stablecoins isn’t just about a voiding systemic risk,” Brookings (Oct. 5, 2021) (available at: <https://www.brookings.edu/research/regulating-stablecoins-isnt-just-about-avoiding-systemic-risk/>) (estimating that as of August 2021 market capitalization of stablecoins was approximately \$120 billion); and Andrew Ross Sorkin, et al., “Here Come the Crypto Rules,” The New York Times (Sept. 24, 2021) (available at: <https://www.nytimes.com/2021/09/24/business/dealbook/stablecoin-crypto-regulation.html>) (estimating that as of mid-September dollar-tied stablecoins in circulation had a value of \$125 billion) (a September 2021 market capitalization of stablecoins between \$120 and \$125 billion represents a 600% increase from 2020).

¹¹ See CoinMarketCap at Tether, USD Coin, and Binance USD, respectively (available at: <https://coinmarketcap.com/currencies/tether/>; <https://coinmarketcap.com/currencies/usd-coin/>; and <https://coinmarketcap.com/currencies/binance-usd/>, respectively) (Jan. 31, 2022).

means of payment.¹² The transition to broader use of stablecoins as a means of payment could occur rapidly due to network effects or the relationships between stablecoins and existing user bases or platforms.¹³

B. Risks Presented by Stablecoins

The emergence of stablecoins pose a bevy of significant risks. These risks are not merely theoretical.¹⁴ With respect to AML/CFT risks, the growth and reach of stablecoins, the degree to which stablecoin arrangements permit anonymity, the usability of stablecoins, the exchangeability of stablecoins for fiat currency, the lack comprehensive regulation of nonbank stablecoin issuers and in stablecoin arrangements, and other characteristics of stablecoins all present risks that must be addressed.¹⁵ The U.S. Department of the Treasury, as a member of the President’s Working Group, has noted these risks and promised to lead efforts to address them.¹⁶ Importantly, there are a number of gaps in how the U.S. currently applies AML/CFT regulations to banks’ payments-related activities and functionally similar stablecoin activities and how U.S. regulations apply to nonbank stablecoin arrangements. FinCEN should modify AML/CFT regulations to address these gaps, particularly given the risks associated with nonbank stablecoin arrangements and their ability to be readily used as a payments mechanism. Specifically, The Clearing House is recommending that FinCEN modify its regulations to address gaps in the four areas discussed in the “Regulatory Gaps Relating to Stablecoins” section below.

¹² “Report on STABLECOINS,” *supra* note 6, at p. 1.

¹³ *Id.* at p. 1 and p. 19 (noting that “[t]he promise of a stable value can, particularly when paired with the reach of commercial firms such as telecommunications or technology providers, increase the potential that stablecoins scale rapidly”).

¹⁴ The G20, for example, has undertaken a study of the risks to the international monetary system presented by stablecoins. See G20, “Assessing the impact of stablecoins on the international monetary system: G20 and IMF to study the impact of Facebook’s Libra project,” G20 Insights (Dec. 10, 2020) (available at: <https://www.g20-insights.org/policy-briefs/assessing-the-impact-of-stablecoins-on-the-international-monetary-system-g20-and-imf-to-study-the-impac-of-facebooks-libra-project/>).

¹⁵ See “Digital Assets and the Future of Finance: Understanding the Challenges and Benefits of Financial Innovation in the United States,” footnote 4, at pp. 3-4 (noting money laundering, terrorist financing, sanctions evasion, illicit finance, kleptocracy, and other risks of digital assets (including stablecoins) and related service providers); and President’s Working Group on Financial Markets, “Statement on Key Regulatory and Supervisory Issuers Relevant to Certain Stablecoins” (Dec. 23, 2020) (available at: <https://home.treasury.gov/system/files/136/PWG-Stablecoin-Statement-12-23-2020-CLEAN.pdf>) (noting AML/CFT risks associated with stablecoins, stablecoin issuers, and stablecoin arrangements). See also “OCC’s Hsu: Stablecoins Can Boost Innovation If Regulated Like Banks,” Pymnts.com (Jan. 15, 2022) (available at: <https://www.pymnts.com/cdn.ampproject.org/c/s/www.pymnts.com/cryptocurrency/2022/occ-hsu-stablecoins-can-boost-innovation-if-regulated-like-banks/amp/>) (quoting Acting Comptroller of the Currency Michael Hsu on “the lack of standards and controls in the crypto space,” as risks associated with stablecoins).

¹⁶ “Report on STABLECOINS,” *supra* note 6, at p. 19 (noting that stablecoins pose illicit finance concerns, including concerns related to compliance with rules related to anti-money laundering and countering the financing of terrorism and proliferation and promising that Treasury would continue to lead efforts at FATF to encourage countries to implement international standards and would pursue additional resources to support supervision of domestic AML/CFT regulations).

C. Regulatory Gaps Relating to Stablecoins

In order to identify regulatory gaps relating to how the U.S. AML/CFT regime applies to nonbank stablecoin arrangements, The Clearing House has examined how such regulations apply to money services businesses (“MSBs”) and has also consulted FATF guidance relating to virtual assets (“VAs”) and VASPs. Nonbank stablecoin arrangements are a subset of VASPs and, according to FinCEN guidance, persons acting as VASPs – as exchangers and administrators of VAs – are generally subject to U.S. AML/CFT laws as MSBs.¹⁷ To address the risks associated with nonbank stablecoin arrangements, the AML/CFT regulatory framework should be modernized to include heightened expectations for VASPs, including nonbank stablecoin arrangements, that bring such arrangements in line with expectations that are presently imposed on banks engaged in payments-related activities, including functionally similar stablecoin arrangements.

1. Customer Due Diligence

Banks and other financial institutions (that are not 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.¹⁸ 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,¹⁹ but as a general matter only MSBs that are providers or sellers of prepaid access are subject to express obligations to have policies and procedures to collect information about a person with which they engage.²⁰ 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.²¹ The FATF Recommendations provide additional detail relevant to this guidance. Specifically, the FATF Recommendations state that financial institutions should be required by

¹⁷ U.S. Department of Treasury – FinCEN, FIN-2019-G001, “Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies” (May 9, 2019) (available at: <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-certain-business-models>).

¹⁸ 31 C.F.R. § 1020.220.

¹⁹ 31 C.F.R. § 1022.210(d)(1)(i)(A).

²⁰ 31 C.F.R. § 1022.210(d)(1)(iv).

²¹ “Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers,” *supra* note 4, 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.*)

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.²² 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.²³

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 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);
- 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; and
- Verify the identity of beneficial owners of legal entity customers.²⁴

2. Correspondent Banking

The FATF Guidance anticipates that VASPs will comply with requirements regarding the management of correspondent relationships and defines “correspondent relationship” for VASPs

²² *Id.* at pp. 49 & 79-81.

²³ *Id.* at pp. 37, 48-50, 52-54, 66, 69-70, 73 & 79-81.

²⁴ The Clearing House understands that FinCEN is expected to issue a rulemaking to revise the existing beneficial ownership rule based on the Corporate Transparency Act, which was enacted on January 1, 2021. (*See* FinCEN, “Beneficial Ownership Information Reporting Requirements,” 86 Fed. Reg. 69,920 (Dec. 8, 2021).)

as the provision of VASP services by one VASP to another VASP or a financial institution.²⁵ 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 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.²⁶ The Bank Secrecy Act also requires additional standards for correspondent accounts for higher-risk foreign banks.²⁷

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.”²⁸ 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.²⁹

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:

- 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

²⁵ “Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers,” *supra* note 4, pp. 52-54.

²⁶ 31 U.S.C. § 5318(i)(1).

²⁷ 31 U.S.C. § 5318(i)(2).

²⁸ 31 U.S.C. § 5318A(e)(1)(B).

²⁹ 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).)

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.³⁰

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.³¹ 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.³²

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.

3. Higher Risk Countries

FATF Guidance provides that VASPs should apply EDD measures to business relationships and transactions from higher risk countries.³³ 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.³⁴ The type of EDD measures applied should be effective and proportionate to the risks.³⁵

³⁰ 31 C.F.R. § 1010.610.

³¹ 31 U.S.C. §§ 5318(j)(1), (2).

³² *See* 31 C.F.R. §§ 1010.630(a)(1)(i) & 1010.630(a)(1)(ii).

³³ “Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers,” *supra* note 4, at p. 66 (Recommendation 19).

³⁴ *Id.*

³⁵ *Id.* at pp. 40 & 43.

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.³⁶ 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.³⁷

To address the risks associated with nonbank stablecoin arrangements, The Clearing House recommends that FinCEN utilize its authority under 31 U.S.C. § 5318A(a)(1) to explicitly apply to nonbank stablecoin arrangements the requirements relating to EDD and other special measures for jurisdictions and entities determined by FinCEN to be of primary money laundering concern.

4. Transparency and Beneficial Ownership

FATF Guidance provides that VASPs should comply with FATF Recommendations regarding beneficial ownership.³⁸ 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.

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.³⁹ FinCEN has issued a notice of proposed rulemaking to implement the reporting requirements.⁴⁰

To address the risks associated with nonbank stablecoin arrangements, The Clearing House recommends that FinCEN proceed with the rulemaking and 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.

IV. Conclusion

Stablecoin arrangements have grown, and will continue to grow, rapidly and present a broad array of money laundering, terrorist financing, and proliferation concerns. It is essential

³⁶ 31 C.F.R. §§ 1010.651-661.

³⁷ 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. (FIN-2019-G001 “Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies,” p. 16, n. 54.)

³⁸ “Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers,” *supra* note 4, at pp. 51-52, 63, 67-68, 80 & 85.

³⁹ The Corporate Transparency Act of 2019 was passed by Congress as part of the Anti-Money Laundering Act of 2020. Additional information on the Anti-Money Laundering Act of 2020 is available here: <https://www.fincen.gov/anti-money-laundering-act-2020>.

⁴⁰ 86 Fed. Reg. 69,920 (Dec. 8, 2021).

the FinCEN modernize the U.S. AML/CFT regime to address the concerns presented by nonbank stablecoin arrangements and ensure that they are subject to the same standards as banks' payments-related activities and functionally similar stablecoin activities. The recommendations set forth in this letter will not only help modernize the U.S. AML/CFT regime as it pertains to the risks posed by stablecoins but will bring the U.S. more closely into alignment with the international standards that the Department of the Treasury supports. If you have any questions, please contact the undersigned by phone at (336) 769-5314 or by email at: Robert.Hunter@theclearinghouse.org.

Respectfully submitted,

/s/

Robert C. Hunter
Deputy General Counsel & Director of Legislative and Regulatory Affairs
The Clearing House Association, L.L.C.

