

January 4, 2021

Kenneth A. Blanco
Director, Financial Crimes Enforcement Network (FinCEN)
US Department of the Treasury
P.O. Box 39, Vienna, VA 22183 USA

Submitted electronically on 1/4/2021 via Federal E-rulemaking Portal: <http://www.regulations.gov>
with copy sent via email correspondence to: kenneth.blanco2@fincen.gov

Re: FINCEN 2020-0020 RIN 1506-AB47 Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets

The Global Digital Asset & Cryptocurrency Association (“GDCA”) appreciates the opportunity to provide comments to the United States Department of the Treasury Financial Crimes Enforcement Network (the “FinCEN”) in response to FinCEN’s proposal to enhance requirements for certain transactions involving “Convertible Virtual Currency” or “Digital Assets” (“Proposed Rule”). While we share FinCEN’s desire to eliminate illicit behavior, remove bad actors, and advance U.S. national security interests, we believe that there are several aspects of this proposed rule which may in fact undermine these objectives. Specifically, we believe that the Proposed Rule in its current form may:

- 1) Undermine the intended advancement of U.S. national security interests;
- 2) Harm the global competitiveness and positioning of the U.S. in the global digital economy;
and
- 3) Inhibit the contribution of the Digital Asset industry to job creation and economic growth in the U.S.

We respectfully request FinCEN to consider these aspects as it works to finalize its ruling.

The GDCA¹ is a self-regulatory association of individuals from over 110 organizations who are committed to advancing good governance, transparency and integrity in the cryptocurrency and

¹ GDCA is a global self-regulatory association for the digital asset & cryptocurrency industry. It was established to guide the evolution of digital assets, cryptocurrencies, and the underlying blockchain technology within a regulatory framework designed to build public trust, foster market integrity and maximize economic opportunity for all participants. Our broad-based membership includes spot and derivative exchanges, proprietary trading firms, traders, investors, asset managers, brokerage firms, FCMs, custodians, decentralized technology organizations, banks, legal firms, audit firms, insurance professionals, academics, consultants, & media.

To fulfill its mission, GDCA devises standards and consensus-based solutions that address the major challenges facing the digital asset and cryptocurrency industry. We collaborate with stakeholders around the world, industry leaders and policymakers to support the growth of the global digital economy.

- Advocate for a regulatory environment that facilitates innovation and protects consumers, stakeholders and the broader public interest world-wide;
- Provide education, training, certification and other resources to build human and technical capacity; and
- Provide thought leadership and facilitate industry engagement.

digital assets sector. Building upon its grassroots-oriented interest and support for the development of a self-regulatory organization (“SRO”) for the cryptocurrency and digital assets industry (the “Digital Assets Industry”), our efforts have focused on operating in an inclusive and consensual manner to set the standards for the Digital Assets Industry and, in so doing, provide guidance for compliant conduct, build mechanisms for the enforcement of such standards, and cultivate the development of the Digital Assets Industry. We are striving to balance the desire for innovation in the industry with the need to protect investors and promote the public interest. At the same time, we are building the credibility, integrity and relationships necessary to effectively align our efforts with government regulators, serve the global community, and support a diverse array of stakeholders.

Given the brevity of time provided for response as well as the importance of this issue, we are deeply concerned that the public comments on the Proposed Rule will lack the number, depth and detail necessary for a fair and thorough evaluation of the Proposed Rule. Additionally this may endanger the integrity of implementation, especially for smaller and newer firms in the space. Furthermore, we question whether this will negatively impact the overall effectiveness of a final rule and create unintended consequences damaging to the interests of the United States (“U.S.”).

Set out below are our views and considerations on the Proposed Rule and our recommendations for further actions by FinCEN.

I. VIEWS & CONSIDERATIONS

Undermine Advancement of U.S. National Security Interests

While we greatly respect and support the need to protect U.S. national security interests, we believe that current AML/KYC Procedures and best practices are more effective than assumed. Additionally, the requirements outlined by this Proposed Rule may not only fail in achieving this desired outcome, but may in fact undermine ongoing efforts to remove nefarious actors and minimize illicit activities harmful to U.S. national security.

In summation, the Proposed Rule seeks to apply existing reporting rules to the Digital Asset industry – and “unhosted wallets” in particular. The Banking Secrecy Act (“BSA”), and the various rules designed to implement the Act, have led to a large body of best practices utilized by good actors and businesses that are based on the concept of “Know Your Customer” (“KYC”) to comply with the BSA (“AML/KYC Procedures”). AML/KYC Procedures are flexible enough to accommodate multiple business models. In addition, no one size fits all. Regulators typically accommodate the need for flexibility in AML/KYC Procedures, allowing participants to fashion their AML/KYC Procedures to best fit their business model, risk profile and size and revenues of the business. AML/KYC Procedures are very effective in mitigating money laundering and other

The GDCA employs a self-regulatory mechanism that is guided by principles of accountability, integrity and transparency to promote the highest professional and ethical standards for its members by developing a Code of Conduct and best practices and holding members accountable via enforcement mechanisms such as surveillance and a legally binding dispute resolution forum. <https://global-dca.org>

illicit activities. Where regulators find deficiencies, the fines and penalties can be huge and, indirectly, serve as a very effective deterrent to other businesses.

To a large extent, the legitimate actors in the Digital Assets industry have adopted AML/KYC Procedures designed to fit their businesses and risk profile. Many organizations are required to register with government regulators, which require the adoption of such procedures. Onboarding consists of a fairly sophisticated system, often overseen by experienced compliance professionals, with the objective of knowing who the customer is, verifying that such customer is not on an Office of Foreign Assets Control (“OFAC”) or Specially Designated Nationals (“SDN”) list, and to establish a profile of the customer for future comparison. AML/KYC Procedures also include appropriate limitations on third-party transfers of Convertible Virtual Currencies (“CVCs”). Participants are also aware of the duty to file Suspicious Activity Reports (“SARs”). Although the industry is still nascent; with knowledge of the potential penalties, GDCA members are highly cognizant of the consequences of the failure to implement effective AML/KYC Procedures.

This is not to say that there cannot be improvements in the Digital Assets industry’s AML/KYC Procedures. Certainly that is the case. There are many CVC-related businesses that are too immature and/or unaware of appropriate AML/KYC Procedures. This fact can be alarming. And yet, a recent analysis of CVC activity demonstrates that the overall proportion of illicit money-laundering activity is very low:

“We see that in 2019, scams made up the overwhelming majority of cryptocurrency-related crime, accounting for a whopping \$8.6 billion in transactions. In fact, were it not for just three separate large-scale Ponzi schemes, the crime would account for just 0.46% of all cryptocurrency criminal activity.”²

In addition, while CVC exchanges continue to be a “popular off-ramp for illicit cryptocurrency, they have taken a steadily growing share since the beginning of 2019. Over the course of the entire year, \$2.8 billion in Bitcoin was traced from criminal entities to exchanges. Just over 50% went to the top two: Binance and Huobi.”³ Neither of those exchanges are based in the U.S. In fact, the vast amount of activity on CVC exchanges occurs on platforms outside the U.S.⁴

Given the rate of adoption of appropriate AML/KYC Procedures by legitimate businesses and platforms in the U.S., the relatively low level of criminal activity that occurs in the markets, and the fact that the majority of illicit activity occurs outside of U.S. jurisdictional reach, the GDCA questions the urgency of the need for the implementation of the Proposed Rules, at least without an appropriate amount of scrutiny and analysis that should be undertaken prior to implementing such impactful regulations.

In fact, in a decentralized and privacy-centric infrastructure, such as is evolving in the Digital Assets industry, requiring the application of existing reporting rules may have the unintended effect of pushing participants to the grey markets, outside of effective U.S. jurisdiction. This may increase the difficulty and ability of regulators and law enforcement to identify illicit activity, eliminate nefarious actors, and further protect U.S. national security interests.

² *The 2020 State of Crypto Crime*, Chainalysis, Inc., January 2020, p.6.

³ *Id.*, p.9.

⁴ See Coinmarketcap’s list of top exchanges by volume at: <https://coinmarketcap.com/rankings/exchanges/>

Harm to U.S. Competitiveness in the Global Digital Economy

But the greater risk to U.S. national security comes from the potential bifurcation of the Digital Asset market and the hindrance of American preeminence in the global digital economy. Further, the cost of implementation for the Digital Asset industry is not considered in the Proposed Rule and its impact may drive bad actors deeper into the dark web, possibly empowering offshore exchanges – some located in jurisdictions adversarial to U.S. interests.

While traditional financial businesses like banks and Money Services Businesses (“MSBs”) have already instituted the necessary AML/KYC Procedures and devoted the required resources to operate, there are many budding enterprises in the Digital Assets industry that may not yet have the resources to implement the required protocols and framework necessary for compliance with the Proposed Rule. The Proposed Rule itself is complex and will take time for businesses to digest and determine how they may comply. The Proposed Rule may, in effect, cause harm to U.S. business development and overall global competitiveness.

The result may be the creation of a different, less liquid, and crippled market here in the U.S., while technological innovation, intellectual property, and global monetary influence is driven overseas. As noted by Ratner et.al. in the Center for a New American Security (CNAS) independent assessment⁵ for the for U.S. Congress as mandated by the FY2019 National Defense Authorization Act, millions of people around the world will soon have access to financial services via blockchain technology and the “companies that develop these applications will control tremendous amounts of user data and have outsized influence on these countries and their relationship with the global financial system.” The assessment goes further noting that the “United States should empower U.S. firms to lead in this space by embracing and encouraging the development of blockchain-based payment applications, both for domestic use and for cross-border purposes. To this end, the White House, in coordination with the Treasury Department, should lead an effort to consider regulatory, legal, and other incentives to promote U.S. fintech development of digital wallet, banking, and peer-to-peer payment applications.”

As one of the highlighted areas within the Proposed Rule relates to unhosted, or self-hosted wallets (an owner has the private key controlling the cryptocurrency wallet and uses it to execute transactions involving the wallet on the owner’s own behalf), it is important to highlight the fact that, the self-hosted wallet solutions serve an important purpose and have broad applications that cannot be achieved utilizing solutions provided by third parties. Self-hosted wallet solutions provide an undisputable element of ownership, control and instant access to funds for the wallet owner without reliance on third parties. These elements are especially essential for institutional investors, regulated entities, and corporate balance sheets as digital assets continue to be broadly considered as an asset class amongst these enterprises. In addition, centralized wallet hosting platforms are not yet able to demonstrate proven and tested controls that can be relied upon by regulated entities. Many sophisticated investors seeking such validation in order to meet internal or regulatory requirements for holding funds at these enterprises, may view self-hosted solutions as providing an important alternative. In certain situations, utilizing self-hosted wallets is the only alternative to demonstrate ownership and control over assets of the account owner needed to pass

⁵ Ratner, Ely et al. “Rising to the China Challenge Renewing American Competitiveness in the Indo-Pacific: An Independent Assessment for US Congress as Mandated by the FY2019 National Defense Authorization Act..” *Center for a New American Security (CNAS)*. (December 2019): 31, <https://www.cnas.org/publications/reports/rising-to-the-china-challenge>

internal and external audits. Imposing onerous reporting and recording requirements on participants utilizing self-hosted solutions hinders broader adoption of digital assets by institutional and regulated participants and may impede the growth and evolution of the industry in the U.S.

While the GDCA fully supports protecting U.S. national security and acknowledges the concerns surrounding unhosted wallets raised by FinCEN, we suggest that more effective approaches are possible, may be better suited for digital asset activity, and may best address the FinCEN concerns identified in the Proposed Rule. One key shift in approach is to focus on the source of funds and the concept of “Know Your Customer” during the KYC/AML onboarding and monitoring process instead of focusing on the means and in effect penalizing a specific solution that is believed to be utilized by bad actors. The GDCA questions whether applying extensive reporting, verification and recordkeeping requirements on the holders of self-hosted wallet solutions is the most effective approach to capture illicit activity and suggests that closer consideration should be given to the source of funds and the risk profile of a customer or a counterparty while evaluating transactions in digital assets. Historically, this approach has proven to be much more effective while applying the BSA and related AML rules for tracing illicit flows of funds within the financial system.

In addition, GDCA wishes to highlight an important unintended consequence of the Proposed Rule and requests its consideration by FinCEN. As the new rule would require banks and MSBs to keep records and file reports with FinCEN of a customer’s CVC or LTDA transaction and counterparty - including verifying the identity of their customer if a counterparty is using an unhosted wallet - this requirement raises undeniable concerns of privacy and physical security for holders of such unhosted wallets. The Proposed Rule requires the collection of at least the name and a physical address of the unhosted wallet holder, which in most cases is also the physical location of the digital assets and the private keys controlling the cryptocurrency wallet. This fact instantly creates a hacking target. As imparted by multiple industry participants to the GDCA, should this information be subject to a security breach - especially within digital asset MSB enterprises which may still be developing their infrastructure - significant privacy, safety and security concerns will arise. Additionally, even if an unhosted wallet owner does not directly transact any activity through an MSB or a bank required to collect certain information, but rather is indirectly connected through the MSB’s or bank’s customer or a counterparty, this presents real concern in the case of a security breach. In such cases, prompt notification to the unhosted wallet owner is paramount but uncertain with respect to the Proposed Rules. The GDCA wishes to highlight the above concerns as an example of unintended consequences of the Proposed Rule, and requests that they are seriously considered by FinCEN.

Finally, if the U.S. is to maintain its leadership position in the global trade and currency markets, it must secure that position by being on the forefront of innovation in multiple areas for digital assets that will evolve over the next 2-5 years. This will require an open framework that promotes industry involvement, global growth and encourages the harmonization of digital asset regulation around the world. In this manner, the U.S. can protect its sovereign institutions and investors, ensure a safe, robust marketplace for interchangeable digital assets, and promote U.S. stewardship of the global digital economy.

Hinder U.S. Job Creation and Economic Growth

During these difficult economic times, it is important to recognize the positive contributions of the Digital Asset industry in job creation and economic growth. Undue burdens as envisioned by the Proposed Rule may have the unintended impact of derailing domestic Digital Asset industry growth, stifling job creation and decreasing economic development. This is especially crucial as a strong U.S. economy is at the heart of U.S. global competitiveness, international standing and national security.

As noted by the 3rd Global Cryptoasset Benchmarking Study⁶ conducted by the Cambridge Center for Alternative Finance at Cambridge University, in the Digital Asset industry, “high-growth companies accounted for more than one out of every four enterprises active in the cryptoasset ecosystem in 2019.” On average, these high growth firms more than doubled their workforce over the three-year period from 2017-2019, experiencing an average increase in employee growth from approximately 84 employees in 2017 to 200 employees in 2019. At a time when the U.S. economy is struggling to navigate the COVID-19 pandemic, economic downturn and severe job loss, additional burdens on industries that have been able to not only survive, but thrive⁷ during these challenging times may not be in the broader U.S. domestic or foreign policy interests.

Further, as an emerging industry, individual entrepreneurs and micro-, small-, and medium-sized enterprises (MSMEs) comprise a significant portion of the industry and are crucial to driving market innovation and growth. In the U.S., small businesses employ 1/3 of the overall workforce⁸ and globally, the Americas region leads as the home to the highest number of overall fintech startups⁹ world-wide. Although large players in the Digital Asset industry exist, a significant portion of industry businesses are MSMEs. While the Proposed Rule may represent a challenge for all firms in the Digital Asset industry, in its current form, it may represent an overwhelming burden for MSMEs. The Proposed Rule could be potentially detrimental to the sustainability of a vibrant and diverse MSME Digital Asset sector in the U.S. forcing firm closure or increased consolidation of control in the sector in the hands of only a few large firms.

⁶ Blandin, Apolline et al. “3rd Global Cryptoasset Benchmarking Study.” *Cambridge Center for Alternative Finance. University of Cambridge Judge Business School.* (September 2020): 18, <https://www.ibs.cam.ac.uk/wp-content/uploads/2020/09/2020-ccaf-3rd-global-cryptoasset-benchmarking-study.pdf?v=1600941674>

⁷ Despite COVID-19, FinTechs continue to grow globally. On average, FinTech firms reported a year-on-year increase in their transaction numbers and volumes of 13 per cent and 11 per cent respectively in Q1-Q2 (used interchangeably with H1 throughout the report). This is consistent with reported improvements in other key market performance indicators such as new customer acquisition and customer retention.

Cambridge Centre for Alternative Finance (CCAF), World Bank and World Economic Forum (2020) “The Global COVID-19 FinTech Market Rapid Assessment Study.” University of Cambridge, World Bank Group, and the World Economic Forum. <https://www.ibs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/2020-global-covid-19-fintech-market-rapid-assessment-study>

⁸ CB Insights. “US Fintech Small Business Report.” https://www.cbinsights.com/reports/CB-Insights-The-US-Small-Business-Fintech-Report.pdf?utm_campaign=smb_2018-11&utm_medium=email&hsenc=p2ANqtz-96YukzDk_aC8RRFmfDHOLpWsN_Aio_Tfl6W8F8UEpmz48cP_7EURRqzVAIjLDVILERC0jRnXkPUtp93JFGKcuZZLu4A&hsmi=67554565&utm_content=67554565&utm_source=hs_automation&hsCtaTracking=2a3744bc-4953-4a35-854d-d36db693c5a6%7C48697594-3e53-4a43-b1b3-0f1dbfe1ab29

⁹ There were 8,775 financial technology (Fintech) startups in the Americas in February 2020, making it the region with the most Fintech startups globally. In comparison, there were 7,385 such startups in Europe, the Middle East, and Africa, followed by 4,765 in the Asia Pacific (APAC) region. [Statista Research Department.](https://www.statista.com/statistics/893954/number-fintech-startups-by-region/#statisticContainer) “Number of Fintech startups worldwide 2020, by region” (November 9, 2020): 1, <https://www.statista.com/statistics/893954/number-fintech-startups-by-region/#statisticContainer>

II. RECOMMENDATIONS

Provision of Typical Time Period (90 days) for Thoughtful Consideration and Industry Response: Although the GDCA has sought to provide broad comments and considerations to this Proposed Rule, as highlighted above and in comment letters submitted to FinCEN by industry peers, the 15 day time period spanning several U.S. bank holidays, in the middle of a global pandemic, leaves only a handful of business days to consider this crucial 72 page notice of proposed rulemaking as well as to provide data-driven, thoughtful and elaborated responses to the 24 individual questions posed by FinCEN. In recognition of the U.S. national security interest inherent in the development of the Digital Asset industry as well as the potential for unintended consequences, which should be researched and debated in an open forum, we respectfully request that FinCEN reconsider its haste and provide, at a minimum, the typical 90-day period for such significant proposed rulemaking.

In addition, we note that FinCEN has established connections and partnerships with industry groups that have been a good source of information and advice which would, in this instance, be able to provide guidance on the subject at hand. On the FinCEN advisory group side, the Bank Secrecy Act Advisory Group (BSAAG) exists to provide industry perspective and practical insight to the application of rules and regulations. We strongly suggest that FinCEN engage the BSAAG on this subject. For its part, the BSAAG would benefit from extending membership to critical elements of the emerging CVC sector in order to focus on key industry or sector issues such as fintech and the Digital Assets industry and most effectively provide guidance on new financial technology (e.g. blockchain, CVCs and Virtual Asset Service Providers “VASPs”).

In addition, it may also be prudent to wait for legislative action on the issue as emerging legislation may conflict with the Proposed Rules. Congress has already started to direct its attention to CVCs, particularly with respect to Treasury-driven digital currency initiatives. In fact, the recent Defense Authorization Act that is awaiting decision from the President contains regulation with respect to the Digital Assets industry. Moreover, earlier this year, FinCEN initiated tech/fintech office hours for the sector—resulting from a strong push by the sector – to ensure they are staying apprised of, and being inclusive of, new technological capacity both for financial services and regulatory compliance.

Additional Clarity and Details Regarding Definitions, Affected Businesses and Reporting Requirements: Although the Proposed Rule contains 72 pages of information, there exist significant areas of ambiguity with regards to the applicability of the rule and the degree and impact on business reporting. It is recommended that additional time, consideration and attention be given to enhancing the precision of definitions, narrowing the scope of firms required to comply with the Proposed Rule, and refining the nature of the reporting requirements to be mandated therein. Further, as the GDCA and other stakeholders strongly embrace U.S. national security and work to promote consumer protection and the broader public interest, it is recommended that FinCEN work in collaboration with the GDCA and industry stakeholders to undertake the necessary research, analyze potential impacts, and develop a clear rule in this issue area.

Longer and Phased Implementation Period for Proposed Rule: Due to the short time period offered for comments, the GDCA cannot provide specific timelines or suggested phases for implementation without a broader consultation across the industry. However, the GDCA would like to raise the issue of utilizing a longer implementation period to support both established as

well as emerging MSME firms with the opportunity to build the processes, systems and procedures necessary to comply with the Proposed Rule. Additionally, the GDCA would like to highlight the opportunity for undertaking a more phased-in approach to implementation of the Proposed Rule. For example, the final rule may consider adopting an earlier compliance date for the USD \$10,000 transaction reporting requirement and later compliance date for the more resource and technically intensive USD \$3,000 transaction recording requirement.

Subsidy or Other Incentive for MSMEs in the Digital Asset Industry to Expedite Alignment with the Proposed Rule: As previously outlined, MSMEs in the Digital Asset industry contribute to a vibrant, diverse sector in the U.S. If the Proposed Rule is adopted, although all firms will be challenged with implementation, undue financial and technical burden will be placed on the U.S. economy's engine of job creation and economic growth – the MSME sector. To alleviate this burden, ensure the vibrancy and competitiveness of the sector, and promote sectoral growth and job creation, it is recommended that FinCEN cooperate with the U.S. Department of Treasury, White House and/or other key agencies to consider how and in what manner either subsidizing compliance with the Proposed Rule or providing other appropriate incentive to MSMEs may defray potential negative impacts.

* * * * *

The GDCA appreciates the opportunity to provide comments to FinCEN regarding the Proposed Rule. If you have any questions about these comments, or if we can provide further information or assistance, please contact Chair of the Public Policy and Regulation Committee, Tony Pettipiece at Tony.Pettipiece@global-dca.org

Respectfully submitted,

Tony Pettipiece, Chair of the Public Policy and Regulation Committee
Gabriella Kusz, Executive Committee

By: The Global Digital Asset and Cryptocurrency Association (“GDCA”)

In addition, the following entities and individuals are also in support of the GDCA's Response:

1. **Straits Financial** - Gene Orr, CEO, Straits Financial LLC
2. **CrossTower** - Kristin Boggiano, Co-founder & President, CrossTower
3. **Illinois Institute of Technology** - Ben Van Vliet, Associate Professor of Finance, Illinois Institute of Technology
4. **A100x** - Nisa Amoils, Esq., Managing Partner A100x
5. **NYSTX** - Ofer Avineri, CEO, NYSTX, Inc.

6. **Overstock.com** - Jonathan Johnson, CEO, Overstock.com
7. **Medici Ventures** - Jonathan Johnson, President, Medici Ventures
8. **tZERO Group, Inc.**, - Alan Konevsky, Chief Legal Officer, tZERO Group, Inc.
9. **AlphaPoint Corp.** - Igor Telyatnikov, CEO, AlphaPoint Corp.

