Monero Policy Working Group (MPWG)
Date: 01/04/2021

Response to Financial Crimes Enforcement Network, 31 CFR Parts 1010, 1020, and 1022: RIN 1506-AB47, Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets

Submitted by: Monero Policy Working Group
Authors: Jayson Benner, CPA, CA; Dr. F. X. Cabañas; Dr. J. Dubois-Lacoste;
Deanna MacDonald; Justin Ehrenhofer;
Dr. R. Renwick; Asst. Prof. Dr. A.J. Santos.
Contact: policy@getmonero.org

Introduction

1. The Monero Policy Working Group (MPWG) is a loosely formed quorum of individuals that contribute to the Monero[1] open-source project. Monero is a permissionless, privacy-preserving cryptocurrency network. The goal of MPWG is to work with regulators, policy makers, and the wider financial services sector to ensure broad understanding of Monero, and other privacy-preserving cryptocurrencies, is communicated. We have specific interest in interacting with entities, so they may understand Monero's component technologies, especially with regards to evolving regulatory framework and compliance requirements. We thank you for the opportunity to respond to the proposed rule - CFR Parts 1010, 1020, and 1022, RIN 1506-AB47, Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets. We give consent for our contribution to be publicly published in full.

2. As we understand it, the period for comments has been shortened for this particular CFR, with 'good cause' being provided as a lawful basis for the expedition. Although we endeavor to give a thorough response, we share the general concerns of others regarding the shortened feedback period. Nevertheless, the MPWG believes the scope of the changes being proposed is significant and, in the interests of fairness and transparency, requires further discussion and consultation from the public.

3. The MPWG welcomes efforts by FinCEN to gather input, perspective and opinion from the wider stakeholder groups found within the sector, especially those that will be greatly affected by this proposed rule change. As the MPWG has not been involved thus far in consultation, we are willing to provide input from the perspective of open-source, permissionless, decentralized, and privacy-preserving projects. While the document mentions a number of events, discussion roundtables, and dissemination seminars have

[1] *see* The Monero Project, https://github.com/monero-project and https://getmonero.org.

already been conducted in order to provide fair and open avenues for debate, it is unclear how many of these efforts have included representatives or contributors from projects committed to serving the public good, based on open permissionless ledgers, such as Monero or Bitcoin, despite such projects playing a key role in the industry.

4. The MPWG understands the mandate of FinCEN is the communicated goal of ensuring national security, financial integrity, and market stability - and comprehends the role of the BSA in ensuring this aim. We also support efforts by entities to provide certainty to the sector, whether through this rule, sector-specific guidance, or supporting regulations. However, there are certain elements of the proposed rule that lack clarity. Without this, we question the degree to which all elements would be efficacious towards the perceived intention.

Risks of Unhosted and Otherwise Covered Wallets Versus Hosted Wallets

5. The MPWG welcomes, in principle, the FinCEN guidance with regards to the definition of *unhosted wallets*: "[u]sers of unhosted wallets interact with a virtual currency system directly and have independent control over the transmission of the value." "When such a person conducts a transaction to purchase goods or services on the person's own behalf, they are not a money transmitter and are not subject to Bank Secrecy Act (BSA) requirements applicable to financial institutions."[2]

6. However, the MPWG would like to first point out that we do not agree with the terminology used for wallets. FinCEN has chosen to refer to self-custodied wallets as unhosted wallets. A definitive feature of open, permissionless cryptocurrencies (CVCs/LTDAs) is that anyone can choose where to hold the private keys to their wallet, including the ability to secure their own keys, if they so choose. Users who hold cryptocurrencies outside of a bank or MSB maintain possession of their own funds, hosting their own wallets and, in many cases, also hosting their own nodes; they are not 'unhosted wallets' from the perspective of the user. Although, for the sake of clarity, this document will retain the terms used by FinCEN, it should be noted that the **MPWG recommends that the terms 'hosted wallet' and 'self-custodied wallet' be used instead.**

7. The MPWG understands that 'unhosted wallets' (and the CVCs or LTDAs controlled within them) function in a manner similar to cash, or other bearer instruments. We acknowledge there are some concerns raised regarding such assets, given their inherent properties of self-custodianship, transaction finality, and transaction disintermediation. For these reasons, we consider the prescription *"by regulation that CVCs and LTDAs are 'monetary instruments', for purposes of the BSA"* overall as *"a reasonable balance between financial inclusion and consumer privacy and the importance of preventing terrorism financing, money laundering, and other illicit financial activity."* In order to ensure an equitable balance, the **MPWG considers it critical that, to the degree the underlying blockchain technology permits, the privacy and fungibility commonly associated with cash be preserved.** To this point, we also feel that if privacy and fungibility were in

[2] *c.f.*, FinCEN 2019 CVC Guidance at pg. 16.

any way undermined by additional reporting requirements and/or transaction graph analysis over and above those currently associated with cash, the balance would then be lost.

8. We feel it should be recognized by FinCEN that complete 'anonymous peer-to-peer transactions' are almost impossible to achieve from both technical and empirical perspectives. **It should be noted that the phrase "anonymity enhanced cryptocurrency (AEC) protocols[3]" should be considered "Privacy Enhancing Technologies[4]" (PET) given that such technologies are commonly used in software to increase security, maintain confidentiality, ensure data integrity, and adequate data protection.** It is unclear why the use of PET in blockchain software requires separate classification as anonymity enhancing; from our perspective, there are considerable risks to consumer protection, market integrity, and privacy if such technology is not deployed.

9. Moreover, **we believe the anonymity of the public key is a necessary precondition for the privacy of the user of a CVC or LTDA.** This was understood as far back as 2008, in the Bitcoin whitepaper.[5] To the degree the anonymity of the public key is preserved, the privacy of the user is protected. However, a crucial point is that this does not require the anonymity of the individual user to be maintained, and this is why the **MPWG supports efforts towards verified identification of bank and MSB customers.** The MPWG understands the merit of the proposed rule, in as much as it does not violate the privacy of the user on the public ledger, while at the same time assists Law Enforcement Agencies (LEAs) in the prevention of terrorism financing, money laundering, and other illicit activities.

10. We also agree with FinCEN that **current methods of transaction (blockchain/ledger) graph analysis, as highlighted in Section II (B)[6], are not adequate to mitigate specific AML/CFT risks**. However, conducting such analysis (usually through third-party proprietary software) leads to a number of risks that are not adequately addressed in the proposed rule. For example, it should be noted that it is entirely possible for criminal organizations to manipulate transaction graph analysis by the physical (off-ledger) theft, extortion, and/or trading (off-ledger) of private keys. It should also be duly noted that it is possible to facilitate money laundering and terrorist financing, while at the same time implicating perfectly innocent law abiding citizens in crimes they have nothing to do with. This ultimately leads to false-positives, false-negatives, as well as potential investigatory bias, as close communities and 'sub-networks' will be more greatly affected if one user (*e.g.*, an alleged criminal) is actively trading with many peers in both legitimate and allegedly illicit activity. Additionally, this has the problematic effect of draining law enforcement's limited resources as they may have to investigate many possible associations (especially if a CVC or LTDA is widely used), while potentially exposing innocent law abiding citizens to unwarranted investigation, harassment and/or, in cases where the alleged criminal activity is serious, potentially life threatening encounters with LEAs.

---

[3] *c.f.*, FinCEN 2019 CVC Guidance at pg. 8.
[4] ISO/TR 23244:2020, Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations, https://www.iso.org/standard/75061.html.
[5] *see* Bitcoin Whitepaper, sec. 10, pg. 6, https://bitcoin.org/bitcoin.pdf.
[6] Limitations of Current Tools to Mitigate the AML/CFT Risks of CVC, pg. 11.

CTR Reporting Obligations

11. The MPWG understands the proposed rule would require banks and MSBs to identify and verify their 'hosted wallet' customers who engage in transactions above certain thresholds and with 'unhosted' or 'otherwise covered' wallets. Furthermore, banks and MSBs would be "required to collect certain information (*i.e.*, name and physical address) concerning the customer's counterparties."[7] There is also an obligation on banks and MSBs to collect other crucial data points, such as timestamping specific transaction ID information. In addition, the MPWG recognizes that a number of reporting requirements are needed to ensure risks concerning AML/CFT and other illicit financial activity are mitigated. Our understanding of this is illustrated in the table below (*see* Table 1).

Type	Sender	Receiver	Reporting Requirement
A.	Unhosted wallet (non-obliged entity)	Unhosted wallet (non-obliged entity)	Exemption applies (Not-within purview of BSA)
B.	Hosted wallet (customer's account)	Unhosted wallet (customer)	Proposed extraordinary recordkeeping requirement over $3000; proposed reporting over $10000
C.	Unhosted wallet (customer)	Hosted wallet (customer's account)	Proposed extraordinary recordkeeping requirement over $3000; proposed reporting over $10000
D.	Hosted wallet (customer's account)	Different Hosted wallet (same customer)	Travel Rule[8] (obliged entities)
E.	Hosted wallet (customer's account)	Hosted wallet (customer's counterparty)	Travel Rule (obliged entities)
F.	Hosted wallet (customer's counterparty)	Hosted wallet (customer's account)	Travel Rule (obliged entities)
G.	Hosted wallet (customer's account)	Unhosted wallet (customer's counterparty)	Proposed extraordinary recordkeeping requirement over $3000; proposed reporting over $10000
H.	Unhosted wallet (customer's counterparty)	Hosted wallet (customer's account)	Proposed extraordinary recordkeeping

[7] RIN 1506-AB47, Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, pp. 13-14.
[8] 31 CFR § 1010.410(f).

			requirement over $3000; proposed reporting over $10000. See paragraph 14.
I.	Hosted wallet (customer's account)	Otherwise covered wallets	Proposed extraordinary recordkeeping requirement over $3000; proposed reporting over $10000
J.	Otherwise covered wallets	Hosted wallet (customer's account)	Proposed extraordinary recordkeeping requirement over $3000; proposed reporting over $10000. See paragraph 14.

Table 1. Reporting requirements of CVC and LTDA transactions

12. The MPWG concurs with the view that CVC and LTDA users in Type A transactions do not fall under the purview of the BSA. While we understand the risk that is posed in maintaining this affordance, we strongly believe that the freedom to transact is well within rational bounds, primarily for two reasons, (i) this freedom is currently afforded to users of cash, and (ii) the affordance ensures a basic level of financial inclusion to marginalized members of society - especially the unbanked, underbanked, or underserved. **While there is a residual risk that remains by allowing Type A transactions, we believe that it is imperative to recognize the important properties of freely allowing funds to be transacted between two willing parties through 'unhosted' wallets.** For clarity, we acknowledge these as being: (i) self-custodianship, (ii) transaction finality, and (iii) disintermediation.

13. The MPWG believes that FinCEN should clearly specify that **the customer's counterparty information should only be required to be reported if it is available, and only if the customer is interacting with its counterparty using the financial institution as an intermediary**. Of course, a risk remains that the customer may withhold information from the bank or MSB when requested, but we feel that this potential risk is covered by existing legislation with regards to illicit financial activity. The MPWG would like to acknowledge that there exists accepted and widely understood reporting requirements for all other asset types and **MPWG welcomes efforts to align reporting requirements of CVCs and LTDAs with comparable assets, such as cash or other bearer instruments**, and we feel that similar reporting requirements should be sufficient for CVCs and LTDAs.

14. We would, however, like to draw attention to the particular transaction types classified as H, and J (*see* Table 1), which we feel require consideration from the perspectives of consumer protection and financial inclusion. In these instances, it may not be immediately possible to obtain the required information *ex-post facto*, for a number of legitimate reasons (*e.g.*, data protection and lack of consent, business confidentiality, decentralized exchange interaction,

smart contract execution, *etc.*). In these instances, there should be clear guidelines in place regarding the proposed course of action regarding (i) customer's counterparty identification, and (ii) the proposed course of action regarding any 'seized' or 'withheld' funds.

15. With respect to the above point, the MPWG would like to state that, in some instances, it may not be possible to clearly identify, in the case of a seizure, where funds should be returned (if they are not to be credited to the customer's account at the bank or MSB). In order to safeguard consumer protection, and protect against potential abuse, clear and transparent guidelines should be provided to the industry from the appropriate government body. Further to this point, the **MPWG urges FinCEN to provide clear and proper guidance regarding the use of transaction (blockchain/ledger) analysis for the purposes of identifying the customer's counterparty - if the information is not forthcoming, or not readily available**. While we recognize that certain analysis techniques may provide considerable information to appropriate entities, without proper safeguarding they can pose risk and potential harm to the individual.

16. The MPWG believes that with this rule change, FinCEN will receive a substantial amount of non-suspicious information on customers who make transactions over $10,000 in CVCs and/or LTDAs. **Unlike with cash and most other assets, self-custodianship of these types of assets (CVCs and LTDAs) is encouraged, common, and recommended by many security professionals.** For example, it is much wiser for an individual to store $10,000 in value within an unhosted CVC or LTDA wallet than it is to store $10,000 in cash at one's residence. Transfers to and from financial institutions by individuals often cover a wider variety of non-suspicious activities than one's typical use of cash, especially as there have been a number of centralized security failures within the sector over the last number of years - some due directly to the lack of oversight by the appropriate bodies. In this regard, we question whether a fair and appropriate balance is provided through this rule change, especially with regards to the thresholds outlined. However, we also understand that the threshold limits are not within the purview of FinCEN, and ultimately a matter for Congress, in conjunction with the appropriate agencies.

17. The MPWG would also like to point to the fact that banks and MSBs are already required to submit Suspicious Activity Reports (SARs) in the case that transactions are deemed suspicious and if transaction amounts are over a certain threshold. The MPWG supports the filing of SARs for suspicious transactions, or other suspicious activities. However, it should be noted that, historically, **CVCs can fluctuate in value more than other types of assets, which could lead to cases of 'risk overestimation,' especially when AML/CFT risk calculation is often catered for by automatic profiling systems and/or algorithms**. If care is not taken to differentiate between cost basis and current value there may be a number of SARs filed on individuals who have merely benefited from asset appreciation in a fair and open market. The MPWG believes that care may be necessary when dealing with CVCs, to differentiate legitimate 'early adopters' from other users with regards to risk profiling.

Expansion of the BSA Definition of "Monetary Instruments"

18. The **MPWG welcomes the classification of CVCs and LTDAs as "monetary instruments," due to the regulatory and tax certainty this accommodates**. However, we are keen to stress the importance of information privacy and the concept of fungibility in this regard. As CVCs and LTDAs are not classified as legal tender, they do not have the regulatory protection to ensure that every unit: (i) is indistinguishable from, and freely interchangeable with, any other unit of same; (ii) is accepted universally as settlement of a debt; (iii) maintains comparative market value with any other unit of same. In order to achieve the above properties in the context of CVCs and LTDAs, as required for a proper functioning monetary instrument to ensure integrity, stability, and an adequate level of consumer protection, **there must be some safeguarding of the underlying data structure to ensure informational privacy**. This seems to be inadequately recognized by both FinCEN and the market in general. This oversight impacts on how the sector should classify assets that deploy specific privacy enhancing technologies.

Request for Comment

19. As a policy working group, we also welcome the request for comment towards specific lines of enquiry. We would like to provide comment on the following:

> ***Has FinCEN struck a reasonable balance between financial inclusion and consumer privacy and the importance of preventing terrorism financing, money laundering, and other illicit financial activity? If not, what would be a more appropriate way to balance these objectives?***

20. It is not clear to this group whether FinCEN has conducted a balancing test between aspects such as those listed above. **We believe that there is both an ethical and legal argument that may be made concerning the intrusion of privacy due primarily to the additional reporting requirements set out in this rule change**. Firstly, it is unclear how a customer of a bank or MSB will obtain (or communicate) consent from the customer's counterparty with regards to the transfer of personally identifiable information to the party required to report it. This is especially troublesome to navigate given the regulatory complexity inherent to non-jurisdictionally bound digital assets and the transnational nature of their transactions. There may conceivably be situations wherein: (i) a counterparty may not be aware that such transfer of data is being made, (ii) the transfer is being made to an entity unbeknownst to them, and (iii) the transfer is to a different jurisdiction to their own residence. **This situation would raise considerable issues concerning legal liability (*i.e.*, data protection) on behalf of the customer, but also for the bank or MSB.** Due care should be taken in this regard, especially given recent rulings concerning international transfer of data by obliged entities.[9]

[9] European Parliamentary Research Service, The CJEU judgment in the Schrems II case, available at: https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf.

21. Furthermore, it should be stated clearly that the main outcome of this proposed rule change would be that banks and MSBs (and FinCEN) continue to accumulate vast silos of information on their customers, as well as their customers' counterparties; their personally identifiable information, transaction details, amounts, destinations, timestamps, consumer behaviour patterns, etc. While this silo would have considerable benefit to LEAs, **it is unclear how FinCEN is intending to regulate the collectors of this data (banks and MSBs) to ensure a fair and proper level of consumer protection and data security is maintained**. There is a considerable discussion concerning the potential for data misuse. This is especially worrisome given the rise of Artificial Intelligence and Machine Learning based techniques for re-identification, price discrinimiation, targeted advertising, and transaction-based behavioural analysis - which of course would have considerable ramifications (both ethical and legal) for market stability, market integrity, and consumer protection[10] [11].

22. Finally, it seems from our short evaluation, that a secondary outcome (perhaps intended) of the amendment is that CVCs and LTDA users would become more inclined to ensure withdrawals made from banks or MSBs are to self-custodied wallets. This would allow them to avoid the intrusion into their own (and their counterparties) privacy. This may in turn, make LEAs and Financial Investigation Units feel they are increasingly dependent on specific transaction graph-based investigatory tools which are often designed, developed, and maintained on a 'for-profit' basis, which both FinCEN and the MPWG have already acknowledged as being unsuitable. The 'for profit' model may considerably skew investigations, as providers of these tools would have clear monetary incentives to communicate certain 'desired' outcomes in order to protect their own revenue stream. Coupled to this, there are also often non-disclosure agreements in place that do not allow proper and fair public oversight and transparency into the algorithms that underpin these investigative tools and the processes that are used to possibly incriminate individuals. Public ledgers are of course open and freely available data sets, but how these specific analysis products interpret this data is mostly unknown. They often use proprietary algorithms that may be imperfect, biased, or based on probability metrics. If these are to continue to be used in investigations, there are both legal and ethical concerns that remain. We urge FinCEN to acknowledge these risks, and provide guidance to the sector to ensure that a fair and proper balance is maintained between consumer privacy and the importance of preventing terrorism financing, money laundering, and other illicit financial activity.

Conclusion

23. As a policy working group, the MPWG supports the proposed rule change, CFR Parts 1010, 1020, and 1022, RIN 1506-AB47 - Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, as we are of the opinion that **CVCs and LTDAs ought to be seen as equivalent to Monetary Instruments for the purposes of the BSA, and the same rules should apply**. However, the MPWG suggests a few changes

[10] Odlyzko, A. (2004). Privacy, economics, and price discrimination on the Internet. In Economics of information security (pp. 187-211). Springer, Boston, MA.
[11] K Bimpikis; A Ozdaglar; E Yildiz (2016). Competitive targeted advertising over networks (pp 561-769). Operations Research, Vol. 64, No. 3.

and clarifications. The use of the phrase 'unhosted wallet' is inconsistent with the traditional functionality of blockchain technology, so a more appropriate term would be 'self-custodied wallet.' In addition, FinCEN should provide a reasoned justification on how the interests of financial inclusion, consumer privacy, and national security are balanced in the proposed rule change given that privacy and asset fungibility could potentially be undermined by additional reporting requirements. Moreover, we agree with FinCEN that current methods of chain analysis are not reliable and often lead to false-positives. Banks or MSBs should be cautioned against depending too heavily on closed-source, for-profit, and potentially discriminatory algorithms. Equally important, the customer's counterparty information should only be required to be reported if it is available, and only if the customer is interacting with its counterparty using the financial institution as an intermediary. FinCEN is encouraged to provide clear and proper guidance regarding the treatment of customer data, in particular how such information should be obtained when it is not readily available. As a technical expert committee, and stakeholder, the MPWG is available for any further consultation upon request.