Kenneth A. Blanco
Director
Financial Crimes Enforcement Network
U.S. Department of Treasury
P.O. Box 39, Vienna, Virginia, 22183.

Comments On RIN 1506-AB47 Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets

Dear Director Blanco,

These comments are submitted in regards to RIN 1506-AB47 which would modify the requirements for certain transactions involving convertible virtual currency.

This request for comments is made on behalf of client(s) of my firm who wish to remain anonymous due to the sensitive nature of the material.

If anyone on your staff would like to discuss the matter further I am available for further comment and can be reached at the contact below.

Sincerely,

James Creech

Contact:
James Creech
Law Offices of James Creech
1921 Page St
San Francisco CA 94117
(312) 469-0883
jcreech@creechtaxlaw.com

Executive Summary

On December 23, 2020 the Financial Crimes Enforcement Network ("FinCEN") issued a notice of proposed rulemaking under 31 CFR Parts 1010, 1020, and 1022. These proposed rules would require money service businesses ("MSBs") to submit reports, keep records, and verify the identity of customers in relation to transactions involving convertible virtual currency ("CVC") or digital assets with legal tender status ("legal tender digital assets" or "LTDA") held in unhosted wallets, or held in wallets hosted in a jurisdiction identified by FinCEN.

As part of the notice of proposed rulemaking FinCEN requested notice and comment from stakeholders who would be effected by these proposed rules. In particular the notice of proposed rulemaking listed twenty-four subjects on which it was seeking further comment. This comment letter is primarily responding to item number four of that list which states:

> "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?"

It is the position of this comment that FinCEN has not struck a reasonable balance between the interests of the consumer and the interest of law enforcement in this proposed notice of rulemaking requirement. The proposed rules overly favor law enforcement because they treat CVC as a greater perceived threat than existing monetary instruments and seek to implement excessively restrictive rules.

Given the unique attributes of CVC, specifically the public nature of the ledger, and the total risk of loss for the holder of CVC, the information requested and the manner in which the information is transmitted and stored by the MSB poses a significant financial, and quite possibly physical harm that outweigh the benefits to law enforcement.

Many of the harms caused the proposed rules cause disproportionally burden CVC users when compared to cash or other bearer type instruments covered by the existing Currency Transaction Reports (CTR) for monetary instruments.

It is the position of this comment that the proposed rules should be abandoned all together. However if FinCEN does promulgate final regulations regarding the reporting of CVC

transactions, the final rules should be modified to better protect consumer privacy and safety as well as to create parity among all CTR's regardless of the form of monetary instrument. The comment recommends the following:

1. Harmonizing the existing monetary instrument rules with the proposed CVC rules including reducing the number of mandatory items required to be reported on the CTR.

2. Eliminating the $3,000 threshold for reporting transactions with self custodial wallets and instead maintain a uniformed $10,000 reporting threshold for transfers from unhosted wallets. (non Financial institution to financial institutions)

3. Further engage stakeholders in meaningful discussion and potential modification of these rules to better facilitate an open and innovative CVC economy by balancing the needs of law enforcement with MSBs, entrepreneurs, and investors.

Part 1 of this comment will discuss why the harmonizing rules between CVC users and traditional MSB users is necessary to create a free and fair financial system.

Part 2 of this comment will discuss individual harms that implementation of the current rules could cause individual CVC users and why it would be improper to impose those harms without a clearer defined set of goals for the proposed rules.

It is impossible to draft these comments without recognizing that FinCEN and the Bank Secrecy Act play a vital role in identifying and tracing illicit funds and bringing wrongdoers to justice. This comment does not want to minimize the role that law enforcement having access financial information plays in keeping Americans safe. It does however seek to remind the agency that every regulation involves making tradeoffs between competing interests. In this situation, the author of the comment believes that the legitimate users of CVC deserve just as much if not more consideration as those that seek to abuse CVC.

Part 1

Shortcomings Of Proposed Rulemaking and How They Can Be Made Better

1. If FinCEN is Going To Require Information Reporting of Convertible Virtual Currency Then it Should be Treated the Same as Other Monetary Instruments

The current proposed rules unfairly discriminate against CVC in three significant ways.[1] First the proposed rules create a new lower threshold for reporting individual CVC users. Second the proposed rules expand the amount of information that must be collected about the counterparty to the transactions. Third the proposed rules expand the information required to be collected to include information upon both the sending and receiving of CVC vs the current rules that only require information on the receipt of monetary instruments.

It is the position of this comment that the rules between CVC monetary instruments and non CVC monetary instruments should be harmonized to the greatest extent possible.

The $3,000 Information Requirement for Individuals using Unhosted Wallets is Arbitrary and Capricious

Currently the $3,000 reporting threshold is only a reporting threshold for transfers from a financial institution (FI) to a financial institution. The proposed rules create new rules that apply to individuals that use an unhosted wallet who transact with a FI by declaring unhosted wallets subject to the FI to FI travel rule and deeming them to be the financial equivalent of an Iranian bank account. There are several reasons why the creation of this proposed rule would be arbitrary and capricious.

A. The Proposed Rules Lack of Evidence Money Laundering or other Financial Crimes is Happening at Amounts Under $10,000

As a new requirement there should be some reasoning in the proposed rules why individual self hosted wallets pose a risk to the financial system that individuals interacting with existing financial institutions do not. While the proposed rules make broad references to the fact that CVC is used to further illegal activities there is no mention of why $3,000 is a suitable reporting threshold when compared to the more widely used $10,000 individual reporting threshold.

In fact the opposite is true. The report makes it quite clear that information is lacking and the proposed rules are being populated partly in response to that lack of data. Both the executive summary and in the background section that lays out the need for these types of reporting

[1] This list is non exhaustive. The author of this comment would like to express his displeasure with FinCEN for publishing proposed rules that drastically rewrite the rules for CVC reporting yet only have a 14 day window for comments instead of the usually 60 day window for comments. Further the 14 day window started late of a Friday afternoon and two of those days are Christmas and New Years days. As such, the 14 day window is really only 8 working days which is not a good faith time period for comments to be drafted, thoughtfully discussed and edited, and submitted.

requirements the proposed rules discuss how difficult it is to quantify illegal activity. For example in the executive summary the estimates of illicit actively range from an industry estimate of $10 billion of illicit activity FinCEN's estimate that $119 billion of activity is "suspicious".[2]

While hard data on money laundering is by definition difficult to quantify, the range of estimates cited by FinCEN uses contain an enormously 10 times multiple. This widespread number leaves the much to the imagination and may speak to both to the CVC industries tendency to understate the problem as well as law enforcement's tendency to criminalize anything that it does not understand. What is clear is the lack of specifics in the proposed rules. There is no mention of specific widespread occurrences of fraudulent activity using CVC only transferred to or from unhosted wallets that tend to occur at the $3,000 to $9,999 level that generating informational reports would help combat.[3]

It is also likely that a lower threshold for reporting will generate a greater number of false positives that will further stretch both law enforcement and MSB providers already thin resources. Proving criminal intent and putting together a case worth prosecuting is far more time consuming at lower dollar amounts because (at least in criminal tax) the dollar amounts have to aggregate to a fairly high level before the sentencing guidelines make it worth prosecuting. This means any number of low dollar suspicious activity will lead to dead ends due to prosecutorial guidelines or the inability to prove criminal activity.

B. The Proposed Rules Ignore the Benefits Unhosted Wallets Provide Legitimate United States Users

What there is hard evidence of, is that unhosted wallets are the safest way to hold CVC and that there are benefits to the 90% of CVC transactions that are not in the least bit suspicious. Control of CVC is defined solely by control of the private key. When a wallet is hosted, i.e. the keys are in custody of an uninsured exchange or at a nationally licensed bank the customer

---

[2] As FinCEN itself notes suspicious does not mean illicit. Also troubling is the lack of US nexus for many of the crimes that FinCEN points to as examples of crimes committed with CVC. Footnotes 16 and 18 are offered as evidence of the problem yet they refer to Chinese nationals and the North Korean Regime as the perpetrators of the crimes. It is unclear how foreign bad actors having to route proceeds through non US MSBs will deter them from committing crimes.

[3] For example a $3,000 threshold might make sense if ransomeware was most prominent at the $6,500 amount and that prior law enforcement actions had found that proceeds were immediately converted to US dollars through MSB's that would be covered by this proposed rules. From anecdotal experiences it seems like most extortion threats that request CVC are under $2,000 and thus would not be subject to reporting under the proposed rules. Again another (anecdotal) reason why this amount is arbitrary and capricious. It is also worth noting that law enforcement would still be able to rely on structuring charges to combat money laundering at the sub $10,000 threshold.

does not actually controls the keys.[4] Since they do not control the key the user only has a credit with the institution notated in CVC and priced US dollars. They have to trust the vendor is going to act in good faith, invest in the latest security to protect the MSB's underlying assets, and actually redeem the credit when it is called upon.[5]

Holding CVC in an unhosted wallet is the only way for an individual to maintain control over the private keys and to own CVC outright. It allows the user to implement security as they see fit including encrypting the keys, securing the keys in "cold" or non internet connected storage, and to pick and chose MSB venders (based upon price, fees, and expectation of liquidity, if they wish to convert to US dollars.

C. The Costs of Reporting at Lower Dollar Amounts Exceed Benefits and May Cut of Legitimate Users From Participating in the CVC Economy

Filing BSA reports is expensive. Given that the proposed rules require more information from filing the reports that what currently is required, and that there is not a sophisticated FI counterparty to automatically supply the information, it is logical that they will be more costly to create than even Suspicious Activity Reports (SAR). According to a 2020 Office of Governmental Accountability study the estimated cost of filing an SAR for a small community bank were as high as $17,773 per SAR filed.[6] While this is an eye popping number, it not cheap for even large institution to file an SAR. Of the 11 MSB's profiled in the GAO report over half estimated that it cost more than $1,000 in compliance costs to file an SAR with the average large or very large bank averaging more that $1,400 per SAR. Three out of the 11 FI in the study estimated that the cost was more the $4,000 per SAR filed.

---

[4] The bulk of assets at exchanges are uninsured. For example Coinbase only carries insurance on roughly 2% of it's assets (ie the "hot" or internet connected assets) and national banks were only authorized to custody CVC in mid 2020

[5] The history of CVC is littered with the bones of once reputable exchanges. Mt Gox is a prime example of how even the most reputable exchange at the time can be a veneer for fraud.https://hackernoon.com/all-cryptocurrency-exchanges-fail-for-the-same-reason-5ds38s8

[6] GAO 20-574 Bank Secrecy Act Table 2 Small Community Bank B Page 47 The author acknowledges that SAR reports are more involved and require subjective interpretation on behalf of the FI employees than at CTR but given that an unhosted wallet will not automatically transmit information like another FI would it makes sense to use them as a comparable costs.

If MSB's had similar costs, and again every expectation is that the costs will be higher given the more rigorous requirements for CVC clients, every single transfer in-between $3,000 and $9,999 to or from a CVC MSB to an unhosted wallet would lose money for the MSB.[7]

The end result of this is that MSB's would not allow users to transfer CVC in and out of their ecosystem to an unhosted wallet unless it was a large enough transfer to justify the compliance costs.[8] Low dollar users would be forced to purchase, store, and sell within a particular wallet provider. The proposed rules could turn CVC into an economic version of Apple's App store where users are forced into a walled garden run by a small monopoly of CVC MSBs.

The establishment of walled ecosystems could have several downsides including the loss of a competitive advantage to foreign exchanges, the risk that the exchanges would behave in anti competitive behavior such as offering a wider buy sell ratio than is available on the open market, and the risk that the exchange would implement predatory fees because existing users would not have an option to transfer CVC to another wallet without paying unnecessary mandatory fees.

This push to require time intensive reporting at lower dollar amounts runs counter to the trend of at least studying raising the reporting thresholds for traditional BSA reporting requirements. High institutional costs of filing an SAR is one reason that many banks and credit unions have requested raising the $10,000 threshold for filing an SAR. The GAO has noted that doubling the reporting requirement would reduce the number of SARs filed by 21% and have a corresponding decrease in the costs of compliance.[9] Thus reducing the threshold for unhosted wallets goes counter to the prevailing trend in SAR administration.

It is the position of this comment that given the three factors above, implementing invasive reporting on small transactions would impose significant burdens on CVC MSB providers and that those burdens would trickle down to individual users. These burdens could potentially lead to consequences such as being frozen out of the CVC economy, having to use storage

---

[7] The lowest cost per SAR in the GAO report was $309. Even assuming this cost for every transfer in and out (which again is illogical) mean that a MSB would have fixed costs that exceeded 10% of a $3,001 deposit that would require reporting.

[8] Another problem with the information reporting is that someone has to police the MSBs implementing and training the procedure. Currently that enforcement is fractured and the responsibility of a number of different agencies. For example credit unions, banks, and broker dealers are all regulated by a different agency. This proposed rule does not discuss which agencies are responsible for CVC MSB compliance and what resources they will need to enforce these rules.

[9] If the original $10,000 reporting requirement were indexed for inflation from it's 1970 enactment the reporting threshold would be $61,276 today.

methods that have reduced security or are potentially fraudulent, or being forced to transact outside the United States. The proposed rules would impose all of these burdens based upon law enforcement's unreasonable perception of CVC users as criminals.

The Proposed Rules Require More Mandatory Information than Other Types of Information Reporting

In addition to being potentially prohibitive for smaller transactions, the proposed rules are discriminatory against individuals using unhosted CVC wallets and CVC MSB providers regardless of amount and as such the proposed rules should be modified for transactions above $10,000.

The amount of information collected by traditional MSB providers has evolved into a flexible system that is designed to provide some information to law enforcement but not as barrier to conducting commerce. By contrast the proposed rules create a formal ridged system that requires MSB providers ask detailed probing questions of their customers using unhosted wallets. If FinCEN does move forward with these rules, they should be modified to provide law enforcement the same information that it receives for traditional monetary instruments and remove the onerous and discriminatory burden on CVC users and CVC MSB providers.

A. Mandatory vs Available Information

The most striking difference between traditional information reporting and those information reports in the proposed rules are the difference between what is mandatory and what is best available information. Traditional monetary instruments work under a best information received, or best information available, policy. Information about the sender is recorded if it is available. If it is not available the CTR can be compiled without the information and the transfer will be processed.

The proposed rules do not allow for the same flexibility with CVC transactions. Counterparty information is mandatory. There is no reasonably available exception for self custodial wallets. Under the proposed rules MSB providers will forced to ask questions to comply with the proposed rules or they cannot process the transaction. This is an onerous requirement for both the sender who is required to divulge sensitive information and for the MSB that has to track down and ask the questions.

Even under the best circumstances it is unclear how the implementation of the system will work given the technology and the permanence of a transaction. Consider the following

hypothetical, the owner of an unhosted wallet wishes to transfer 1 Bitcoin to a wallet they control but hosted at an exchange. They wish to convert the Bitcoin into US dollars. They complete an online informational form but fail to complete a required section such as the physical address. The owner then transfers the bitcoin using open source (i.e not the exchange's own website) software directly to the public key of the hosted wallet which bypasses some of the exchanges required fields. After the transfer the exchange realizes the information was incomplete but they are unable to prevent the transfer from taking place. At this point the exchange has limited options because they are in custody of the Bitcoin. They can either 1. try to reverse the transaction by sending the bitcoin back to the public address of the wallet that sent the coin.[10] 2. Impound the Bitcoin until the information is provided.[11] or 3. Retain what information they do have, process the transaction, and risk a fine for failure to strictly comply with the reporting requirements.[12]

Since CVCs do not require both parties permission to send or receive CVC from unhosted wallets, and there is no way to cancel or not accept a transfer like there is for a wire transfer, what to do with unsolicited funds is not exactly clear.[13]

This inflexibility will hinder CVC use and growth in the CVC economy. Making CVC harder to use in the US will open the door for other countries to become the banking leaders in digital currency. This loss of leadership will cost the US jobs because those that care passionately about CVC will immigrate to continue their work.

B. The Proposed Rules Ignore the Importance of Existing Safeguards

One rational for implementing asymmetrical information requirements like FinCEN is proposing with these rules is that in a traditional transfer the counterparty is a FI that maintains information on it's users and self custodial wallets do not. As such the unhosted wallets operate at a privacy advantage compared to a traditional monetary instrument user and this is why heightened information is needed. What the proposed rules fail to take into account is

---

[10] This has a risk of loss because the owner might not realize the bitcoin has been returned and dispose of the private key for an empty address and the institution would have no way of knowing the address has been abandoned.

[11] This creates a problem with a state level conversion claim, custody of the property, and the chance it is never claimed.

[12] Another set of questions arise should the owner be able to convert the Bitcoin into US dollars and transfer the funds out of the exchange before the faulty CTR is flagged.

[13] The end result may be, much like in the smaller dollar transfers that it is easier not to accept transfers from outside the MSB platform.

why CVC users choose to use a particular vendor and how those uses make the existing know your customer information more useful to law enforcement.

For the most part US CVC users use a US based MSB in order to covert their CVC into US dollars. This will not change regardless of reporting requirements. However the digital nature of CVC means that should these rules be implemented privacy oriented users can vote with their feet and opt out of the US system regardless of their motive or physical location.

Without a global system of information reporting CVC users can still convert CVC into legal tender. U.S. based institutions have an advantage in that they are subject to U.S. fraud regulation and are for the most part secure and reputable. However, those advantages have their limits. If regulation makes transacting with U.S. based MSBs more costly and complex then future exchanges and CVC users will move elsewhere and U.S. based MSBs at a competitive disadvantage. U.S. users can still obtain U.S. dollars abroad and have them wired back into the U.S. without disclosing CVC holdings.[14] Foreign criminals can still target U.S. citizens or launder money using CVC. Directing crime away from the United States does not reduce the overall amount of crime and may drive it to jurisdictions were the authorities are less able to counteract the underlying harms.[15]

When determining what kind of burden is placed on CVC users and CVC MSB's FinCEN should take a look at how CTRs are used and how effective CTR's are in fighting crime.[16] Just as the proposed rules state that law enforcement blockchain monitoring is not a panacea for crimefighting neither are CTRs. CTRs or other BSA reports are useful but they require context within the larger wrongdoing and more often than not they are used to confirm cash flows after the underlying wrongdoing is discovered. Narrower CTR criteria, plus adding other reporting will have more of an impact on illicit funds than requiring burdensome CTRs for CVC

---

[14] Even if foreign exchanges become subject to FBAR reporting the amount of information required to be reported is limited and foreign wires from exchanges would not contain sensitive information about CVC addresses (addressed in Part 2)

[15] For example money laundering to finance terrorism is harder to disrupt when it takes place in Dubai and without the IRS's ability to track CVC (thanks to U.S. nexus) the Welcome To Video network would still operating in South Korea and would still be abusing children.

[16] Two GAO reports of note, GAO 20-574 and GAO 19-582 detail systemic problems with how FinCEN communicates Bank Secrecy reports to law enforcement. Some surprising numbers from these reports. 41% of FBI drug enforcement actions did not use BSA information at all. There is very little use of BSA information by state and local law enforcement. One of the law enforcement agencies, IRS Criminal Investigations, that did extensively use and track information provided by FinCEN only initiated roughly 500 investigations a year from BSA reporting and only 60% of those lead to a referral for prosecution. Unsurprisingly the GAO notes that many of the limitations come from agencies lack of staffing and lack of resources.

transactions. After all, it is the matching and confirming of cash flows from different sources that prove the crime beyond a reasonable doubt.

Lighter but expansive reporting across several financial fronts is what Treasury should be focused in light of the limited resources of law enforcement. One example of this multi factor reporting would be to scale back the CTR requirements and introduce a unified CVC income or transaction reporting requirement such as a 1099-CVC (complete with basis). This would generate more information on US based taxpayers who convert CVC to US dollars at a relatively low administrative and compliance cost. Plus it would generate revenue as opposed to the current CTR proposal which is solely an expense.

Another alternative that could provide the government information it needs to track criminal activity is to enter into information sharing agreements with U.S based exchanges. If MSBs who offer custodial services (who would be the most important MSB information providers under the current proposed rules or these revised recommendations) published a list of their public custodial keys that would allow law enforcement to quickly identify a particular MSB as a recipient or sender of CVC. Law enforcement could then request information from the known MSB relating to the account holder who received the account credit, or get a warrant for the know your customer information. For example, an ATF agent identifies a suspicious CVC transaction. The recipient of the transfer is public address that is a known address of MSB Y based up their bi-weekly self identification of public addresses. The ATF agent can make one request and get the name, address, email address, and drivers license of the person who was credited as sending or receiving the CVC. This would be a simpler way of getting information as opposed to using a CTR and having aggregate public custodial addresses would limit the user harm discussed in Part 2.

The Proposed Counterparty Information is Too Broadly Defined

The most important difference between the proposed CVC rules and the existing monetary instrument rules is the breath of information required from the counterparty.

One example of the breath of this rule is the requirement that the MSB make detailed inquiries to the senders (or recipients) information including name and physical address along with type of CVC, U.S. dollar amount, and CVC address. If requested by law enforcement this information would be supplemented by other know your customer information such as email address, social security number and so on.

The first thing to acknowledge is that some of this information would be difficult to obtain. As a permissionless currency, CVC does not requirer users to have physical addresses. In fact one of the advantages of CVC is that it allows people who cannot bank because they lack a permanent address or drivers license access to a financial asset. Requiring counterparties to make inquiries into the background of the people that they transact with on the internet places an unfair burden on users and will effectively make CVC's similar to traditional bank accounts where there is an entire class of people that are blacklisted from conducting transactions because they do not fit the regulatory criteria.[17]

Another reason that the counterparty information is too broad is that information provided would allow the holder of the information to reconstruct a CVC holders CVC history to an extent far greater than if cash or other bearer instruments were used. Assets on the blockchain rely on an agreed upon ownership history. An blockchain address used to transfer CVC to a MSB could be used to track the CVC back to the date and time that it was mined as well as the place in time in the future where it is eventually sold and spent. This could potentially allow interested parties to reconstruct a number of sensitive items such as net worth, contributions to politically affiliated groups, transfers to charities, etc.[18]

CVC tracking is not limited to forensic specialists either. Software such as Cointracker make it easy for any interested party to search the blockchain. Coupled with name and address it becomes possible to add context to each transaction and draw a fuller picture of who, what, when, and why a transfer was made. While the second order effects are discussed more in Part 2, it is important to contrast how this differs from traditional monetary instruments.

If we use two examples of two different CTR (or for the sake of arguments to SARs) the disparities in type of data collected is very clear. In example A a CVC user sends half a Bitcoin they have owned since it was mined in 2015 (as part of a reward of 25 bitcoins) to themselves from an unhosted wallet. Under the proposed rules they would have to provide their own name and physical address to the MSB as part of the compliance procedures. The MSB now knows who the are, where they live, and what their public key is. If the MSB and it's employees do

---

[17] This blacklist would perpetuate the chronic problem that it costs more to be poor than it does rich. For example, sending money via a storefront money transfer system is magnitudes more expensive that sending a wire.

[18] Not discussed in detail in this comment but worth a mention is the chilling effect on speech and freedom of association this might have. For example if a donor made gifts to a politically unpopular group using CVC there might be repercussions if it was discovered. Or if a foreign national used a U.S. MSB to transfer funds to a group that was blacklisted in their home country and then that information was shared with their government. For example a Saudi national uses a U.S. MSB to provide CVC to a women's rights group and the Saudi government gets a copy of the CTR report they might then imprison or execute the donor.

any basic tracking they know the user has assets of at least 25 times the current FMV of bitcoin (which at January 4, 2021 prices would be $775,000) even though there has been no transaction other than transferring assets from one pocket to another.[19]

This is a much clearer financial picture of who the user is when compared to a cash transaction where no counterparty information is required. If we take example B where a MSB customer sells a car for $30,000 cash and takes it to the bank to deposit. The bank records who deposited the cash and some basic information like their address and bank account number and makes the deposit. Unlike the CVC situation does not require the name of the person who bought the car, the person making the deposit to identify other bank accounts they have signatory power over, nor do they have any idea of the basis of the car was.

It is our recommendation that the blockchain address be removed from the criteria to be included on the CTR and instead replace it with the MSB account number of the user.[20]

Other Collateral Concerns

The Technology Has And Will Continue To Move Beyond Traditional MSB Providing Structure

CVC is still in the early stages of development. As the technology develops use cases will be created that might inadvertently subject unanticipated users to MSB requirements. One example of this that already exists is the Bitcoin Lightning protocol. Bitcoin Lightning is a technology used to shortcut Bitcoin's relatively slow settlement speed of 10 minute block confirmations. Bitcoin Lightning solves this problem by creating open accounts that allow for pre confirmation of the transfer ahead of the block being published and confirmed as part of a larger node.

For many retail venders, for example a coffee shop or a book store, using the Bitcoin Lightning protocol allows them to accept CVC which they would not be able to otherwise. They may also be tempted to run a node on their business computer in order to speed up the transaction and reduce fees. The problem comes that if they do run a node there is a chance, should the

[19] At the valuations on January 4, 2021 the total value is 25 x $31,000 or $775,000.

[20] This would better match industry standards at some of the larger exchanges. The account numbers could serve as a stand in for the blockchain addresses until some particular suspicion was identified and then the blockchain addresses are easily requested with a warrant. This extra step is a small price to pay for preserving users safety as discussed in Part 2

proposed rules become final that they would inadvertently become a MSB and have to collect detailed information on all of their customers who used an unhosted wallet.

While this example is a limited one, and the operator of the Bitcoin Lighting node in this example would most like not encounter transactions above $3,000 or $10,000 it is an example of how difficult it is to anticipate innovation in this area. Frictionless payments have only become more important in our post COVID world and effectively cutting of development of new technologies by placing costly compliance burdens does not further US economic growth.

In addition, these rules do not address how these rules impact decentralized finance (DeFi) where there are no addresses or people that can be specifically identified by a contact and contracts are automatically executed. DiFi is poised for enormous growth in the next few years and could be a source of dramatic innovation and growth for the United States economy. It is unclear if these rules will require a clean break from the existing CVC economy because of the lack of required information and what that will to push innovation outside of the U.S.[21]

Part I Summary

Well crafted regulations are narrow and don't create unanticipated second order consequences. These regulations have a number of unintended consequences from excluding users from participating in the CVC economy to potentially creating CVC MSB monopolies and exposing CVC users assets. As a result they are over broad and FinCEN should take a second look at how to better match CVC reporting so that it is only as broad as the existing reporting for other monetary instruments.

Part II

Impact on Legitimate CVC Users Life, Liberty, and the Pursuit of Happiness

As noted in the executive summary, the real burden of these proposed regulations falls on individuals. While MSB providers are the ones charged with implementing these proposed

[21] This comment is not going to address DiFi directly because there is too much to say given the space and time constraints. However it would be unfortunately if these proposed rules forced talented technicians and entrepreneurs to other countries.

rules the costs and privacy concerns are ultimately born by CVC users.[22] While request for comment item four discusses "Financial Inclusion and Consumer Privacy" it is the opinion of this comment that those terms are far too sanitized to represent the true consequence for individuals should these proposed comments become final regulations. Some legitimate CVC users will suffer dramatic loss of privacy that could threaten their economic liberties, and potentially they and their families personal safety.

1. The Blockchain is an Open Economic System and Anonymity Protects Good Actors More Than it Shields Bad Actors

A. Ownership of CVC relies on an open platform where ownership of assets is agreed upon by all participants. As a result the blockchain and all of the transactions are visible and searchable. All transactions are immutable and prior transactions are preserved for posterity. Since each unit of CVC is unique each transaction is not only marked based upon its past history but is trackable for all future transactions as well. The end result is that anyone who is interested can track a transaction.[23] All they need is a reason why. For some users that "why" is to learn more about the asset, to track stolen goods. For bad actors that "why" would be to connect large CVC accounts to individuals based upon the history of a public key so they can be targeted either in person or online and robbed.

The practical result of this is that certain blocks in the blockchain have more interest than others. Astute observers have carefully kept an eye on the origin blocks owned by the anonymous creator of Bitcoin, Satoshi Nakamoto, in case a transfer occurs that can shed light on who this man of mystery really is. Likewise earlier in 2020 an account tied to the Silk Road criminal marketplace moved for the first time since 2015.[24] The movement of the coins was first reported by private blockchain observers and within a matter of hours the IRS and other

---

[22] This is true even if the only cost was increased compliance costs. These costs become fees ultimately paid for by the user. However it is the position of this comment that increased user fees are the least of the end users concerns.

[23] Software has made tracking transactions easy. It does not require any technological skill to become a bitcoin Sherlock Holmes or accurately report basis, holding period, and gains on a tax return.

[24] Another example is this website that tracks the bitcoins stolen from Mr. Gox https://www.cryptoground.com/mtgox-cold-wallet-monitor/ It is not hard to imagine a similar database created out of public keys, numbers of coins being held, last transaction date and time but with real users names, addresses, and phone numbers being circulated if the CTR repositories suffer a data breach. After all, the Mx. Gox database was created by one user with a vendetta and a legal claim. A target list could potentially have dozens of contributors able to post detailed information.

federal law enforcement agencies were forced to issue a press release stating that they had tracked down, had control over the wallet, and had seized the coins..[25]

As public as the blockchain is, there is one piece of information that keeps many of it's users safe from being targeted for their CVC assets. The name, address, and other identifying information of the owner is not part of the public transaction. It is impossible to tell who owns a block of coins that was mined in 2011 that might now be worth $500 million dollars if the blocks have not moved since they were mined. Likewise it is impossible to tell if a specific block of coins is owned by a high profile person such as an athlete, tech investor, or politician. This thin veil of anonymity is all that prevents high net worth, or high profile individuals from become targets of CVC theft.[26]

Anonymity as protection for legitimate users is not something that should be treated lightly because CVCs have a risk of loss that is greater than any other asset. Ownership of CVCs is based upon the control of a private key. If that private key is compromised via hacking, loss due to carelessness, or a computer crash there is no way to retrieve the CVC that it controls. There is no way to recover CVC that was transferred to the wrong address or embezzled by an exchange. This risk of loss leads many technically capable users to rely on self hosted wallets to safely maintain their private keys because they feel safer when they are responsible for their own security or don't trust MSBs to safeguard their assets or personal information.[27]

If we use FinCEN's own estimate of suspicious activity as a proxy for legitimate users vs criminals then legitimate users comprise 90% (or more) of the CVC activity.[28] This means for 9

---

[25]https://www.justice.gov/usao-ndca/pr/united-states-files-civil-action-forfeit-cryptocurrency-valued-over-one-billion-us

[26]It is important to remember anonymity is not unique to CVC. Cash offers anonymity. So do corporate formalities. Online discussion is based on pseudo anonymity. What makes anonymity special in the CVC context is that is just as easy to transfer $1,000,000 as it is $1 and that is difficult at best for governments to implement control over the ability to transfer. It is also important to remember that it is not illegal or immoral to own CVC and given how difficult it is to use CVC to purchase necessities such as food, housing, or telephone/internet services means that CVC is less likely to be used for illicit activities as paying employees under the table, or for retail illegal drug sales all of which have a high aggregate dollar amount.

[27] This can be done in the form of a file on a desktop, a purpose made crypto wallet, or even a flash drive in a safety deposit box. There is a saying if you don't control your keys you really don't own your crypto. This saying has a ring of truth to it because if an exchange has the keys all you really have is a credit with the exchange and if the exchange collapses you have nothing but a creditors claim.

[28] In reality is it probably more because investors are more likely to buy and hold as opposed to buy and transact in CVC and are therefor under represented in the total number of transactions. This ratio has between legitimate users and criminals has most likely been increasing (more legitimate users) because it has become much easier to buy CVC using retail platforms such as brokerage accounts.

out of 10 users anonymity protects them against criminals not law enforcement. Rolling back the main form protection they currently enjoy is not something that should be done lightly. The needs of the majority should be balanced against the needs of law enforcement in prosecuting the few.[29]

Finally anonymity is an integral part of how the blockchain functions. Since all addresses are nominally the same they are all given roughly the same priority for processing. Unlike the stock market where small retail shops can route their orders to high frequency traders that use that information to make a fraction of a penny front-running each trade, all blockchain transactions from the largest MSB to the smallest investor are only judged on when the block was transmitted and perhaps a willingness to pay a larger fee. This prevents block confirmation discrimination. If this mass anonymity, for example by a leak of every user who as interfaced with a U.S. MSB, was ever sacrificed it might threaten the entire blockchain and the ability to transfer any assets.[30]

Anonymity is Not Absolute and Law Enforcement is Policing CVC Activity

There are some limits to anonymity. CVCs are not completely anonymous if placed within the context of events outside the blockchain and users are free to publicly identify themselves and the type and amount CVC they own. Law enforcement in particular has become adept at de-anonymizing CVC and using that information to arrest and convict wrongdoers. For example the IRS has employed technologically advanced techniques to disrupt sophisticated criminal syndicates such as the Welcome To Video and it's users by analyzing and tracking blockchain transactions, and the IRS has arrested and prosecuted US based mixing services and tax evasion.[31] The Department of Justice has also announced inducements against a number of

---

[29] There is always the risk that making it easier for criminals to commit crimes by giving them a wider selection of targets will increase the overall rate of crime perpetrated by criminals seeking CVC

[30] This type of leak would immediately and perhaps permanently decimate the price of the CVC that suffered the leak. Demand may never recover because a large percentage of the CVC would forever be linked to particular identities and that would prevent new parties from either accepting the CVC or be willing to conduct arms lengths transactions when they know their own identities could be at risk in the future. Given the large market cap of Bitcoin and the amount of unrealized gains due to recent price appreciation one would be hopeful that Treasury would not take too great a risk with billions of dollars of future tax revenue.

[31] https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child
https://www.justice.gov/opa/pr/ohio-resident-charged-operating-darknet-based-bitcoin-mixer-which-laundered-over-300-million
https://www.justice.gov/usao-wdwa/pr/former-microsoft-software-engineer-sentenced-nine-years-prison-stealing-more-10-million

individuals for crimes such as running a CVC based Ponzi scheme as well as failing to implement know your customer requirements for CVC MSB providers.[32]

The end result of this is that while it might be harder to detect the underlying crime once the crime is discovered it is easier to prosecute. The immutable nature of CVC makes it easier to document when an illegal transaction took place, and how much it was worth. If law enfacement is able to continue advancing it's technological ability to track and de-anonymize CVC using existing requirements like know your customer information we may see a shift in criminals desire to use CVC even without subjecting unhosted wallets to BSA reporting.

B. De-Anonymizing All Users To Catch Criminals Places Legitimate Users At Risk

If these proposed rules come into effect it will drastically increase the number of people who know about individual CVC users unhosted wallets and what types exchanges of CVC for legal tender they have undertaken.

It is hard to overstate the risks that individual users face should this information become public. It is also hard to overstate what kind of target this information will become for sophisticated criminals. In plain language if the proposed rules do not make any changes to the reporting requirements the CVC CTRs will become a target for some of the most sophisticated bad actors on the planet. Once they have the information they will then use it to specifically target and steal CVC from individual users which will cause enormous economic harm.[33]

Given that this information will be transmitted and stored electronically, CTR reports will be a prime target for hackers. Hacking can happen to both the MSB venders who compile the records, and to the government who receives the report. Of the two hacking of MSB venders is the more likely. For many CVC MSBs compliance is an unwanted department. It is a cost center not a money maker. That means it does not get the best resources the company has to offer and can be overlooked by management. Hacking the CTR reports stored in an internal network is bad but does not threaten the existence of the MSB like losing the underlying CVC.

---

[32] https://www.justice.gov/usao-sdny/pr/founders-and-executives-shore-cryptocurrency-derivatives-exchange-charged-violation
https://www.justice.gov/usao-nj/pr/three-men-arrested-722-million-cryptocurrency-fraud-scheme
https://www.justice.gov/usao-sdny/pr/cryptocurrency-founder-bruno-block-charged-multimillion-dollar-tax-evasion-scheme

[33] Again it is difficult to overstate the type of loss CVC users face. It is unlike anything a W-2 employee with an FDIC insured bank account and a SPIC insured brokerage account who pays for day to day expenses with a credit card faces. Making it even harder to bear is that most CVC users have highly concentrated their net worth in CVC assets. It is possible for CVC users to go from multi millionaire to broke in a matter of minutes.

However, for the individuals who's names, address, and unhosted wallet address get compromised the consequences could be dire.

The same goes if Treasury is hacked. Recently Treasury was hacked using compromised Microsoft certs issued through SolarWinds.[34] It is still unknown who hacked Treasury but it appears that it was a nation state. If it happened again, and CVC CTR reports were compromised, it would not be a stretch for a rouge nation state like North Korea, Iran, or Russia to begin tracking the addresses associated with the CTRs to find the large CVC holders. They could then target those holders computers in an attempt to find the unhosted wallet keys stored on a personal computer or cell phone. With the resources of a nation state individual CVC users security would be overwhelmed and they could face a total loss of their CVC assets.

A lesser appreciated threat comes from individuals within MSB providers and Treasury. A disgruntled employee might find it lucrative to access CVC CTR reports in order to obtain the name and address of large CVC holders. Likewise organized crime might pressure or bribe employees to do the same in order to get a list of names and addresses that have multiple CTR reports filed during a year.[35]

The recent history of cybercrime has taught us that if the information is valuable people will try to steal it and CVC information is more valuable than typical financial information. More often than not they are successful. As a result the only foolproof way to protect user identification is not to create the data in the first place. Information does not simply exist in a vacuum for only the good guys to use.

Another set scams targeting CVC users could originate outside of the central repositories but nonetheless use the required CTR information as a way to perpetrate fraud. If the burden of reporting the counterparty falls to the end users, it could potentially cause a proliferation of scams that use the reporting requirement as a facilitator for fraud. For example, Fraudster A targets User 1, Fraudster knows User has a booming business sells self created products (such as art, handicrafts, or personal services such as building websites) online. That User operates under a pseudonym, and only accepts CVC. Fraudster purchases some of their goods using CVC and tells User that they need compliance information to send the purchase price. Once they have the information, instead of sending payment they start extorting User 1, or other

[34] See also the Office of Personnel Management data breach in 2015. This was also most likely carried out by a nation state.

[35] Nation states have already employed technology employees to spy on dissidents. It is not unrealistic to think that large scale organized crime might do the same. https://www.justice.gov/opa/pr/two-former-twitter-employees-and-saudi-national-charged-acting-illegal-agents-saudi-arabia

purchases or User 1's goods by tracing the CVC address and the transfers to the address, by threatening to contact law enforcement with made up claims of tax evasion or other claims.[36] Under the current rules this type of crime is impossible yet the proposed rules open the door to bad actors.

C. Once an Identity is Linked to an Address the CVC Holder Faces a Number of Risks

Since CVCs transfers are irrevocable, and it is easy to move CVC internationally, CVC assets are high value targets for hackers, fraudsters, and thieves. Each of these criminals have their own method of attack yet the commonality is that each target is the individual not the blockchain itself.

Hackers seek to get unauthorized access to computer systems to see what information they can obtain. This is done a variety of ways including brute forcing passwords, accessing unprotected systems such as printers, or in the case of SolarWinds exploiting a vulnerability in the software itself. The risk from hackers comes not from them attempting to guess or brute force an attack on the private key itself but it comes from gaining access to the CVC users computers, phones or other trusted devices that story the keys and then transferring the keys to themselves. Then they can use the keys to obtain the underlying CVC.

Fraudsters use phishing or other deceitful methods to gain access to computer devices. The sophistication of phishing attempts improves dramatically with the reward being sought. The threat level to identified CVC holders is magnitudes greater than the run of the mill "Your nexflix account has been canceled" emails that contain poor grammar. Once a name is tied to an identity the phishing attempts become much more personalized and specific. This means they are more effective and users suffer greater losses.[37] Once they gain access they can ether steal keys or install ransomeware and demand payment to restore the device. Thieves can steal cell phones or steal access to cell phones via sim swaps to bypass security measures such as two factor authentication. Even milder threats, like being doxxed, can lead to harassment, property

[36] This scam becomes more meaningful if the artist is in a repressive country and the art is political. It also is scalable in User has some access information for past clients like they build the website and then act as administrator and have administrator credentials.

[37] Frequently CVC phishing attempts use the identifiers have been leaked like CVC exchange, account numbers, false transaction data, and can mimic the url of the exchange. It takes a great deal of discipline to not click the link that purports to resolve a crisis.

damage, and having to routinely change phone numbers and email addresses to maintain some semblance of private home life.[38]

Regardless of the tools these criminals use, once they have an individual as a target the individual is no longer safe online and the online world is increasingly blending into the real world. Every day actions like logging into email, or setting up a new internet device that uses their wifi network is fraught with risk. Passwords have to be continually changes and multi factor authentication must be used. Even then there is no guarantee of safety. Resilient and determined criminals, especially ones with nation state backing, are likely to succeed in getting access to any device that has an internet connection. As a result there is a sizable risk of loss if an individual's name were to be released along side a public key.

Computer crime is not the only risk that identified CVC users face. If the CVC holdings are sufficient enough their personal safety might be at risk as well. CVC holders have been subject to a number of (non US) kidnappings where individuals have been held for CVC ransom.[39] Kidnapping is more likely involving CVC holdings is that there are fewer safeguards to prevent the ransom being paid. CVC is a twenty four hour a day market and transfers can be made directly from the person who is kidnapped to their kidnappers without it having to go through a banker or FI who might recognize that the transfer is being made under duress and follow instructions or contact authorities.[40] Likewise criminals might be encourage to commit burglaries or home invasion robberies if they think they can net millions of dollars in CVC by threatening the personal safety of the user and the user's family by using violence to obtain the private keys.

Part II Summary

Given all their attributes CVC assets and their users capture our imaginations. For some the word Bitcoin conjures up images of wealth and luxury living. For others it brings to mind criminals and dark conspiracies. As easy as it is to get caught up in the image, for many people who are actually involved with CVC they are just an asset that requires a great deal of personal responsibility to protect even as they live an otherwise ordinary day to day existence.

---

[38] Doxxing is where a person's name and contact information (address, phone number, email) are published online will an incitement for other people to contact them with harassing messages. This might happen for example if CTR data is used to link CVC users to donations to political causes.

[39] https://cointelegraph.com/news/singapore-crypto-consultant-kidnapped-for-1-million-ransom

[40] Again this is highly correlated with the 100% risk of loss. No-one is going to kidnap Warren Buffet and expect him to surrender ownership of Berkshire Hathaway stock because the company would not recognize the transfer of the stock as a legitimate transfer. However a forced transfer of CVC is still an effective transfer and cannot be reversed.

The challenge when it comes to regulating CVC balancing the needs of the average user at the same time an agency is regulating the edge case. For law enforcement catching criminals on the dark web is hard but glamorous work. Bringing down the Dread Pirate Roberts can make a career. This push to make the bust makes it easy to lose the forest for the trees. Good regulations don't overburden millions in order to catch a handful of criminals.

Unfortunately this is what these proposed rules do. They place excessive burdens on self hosted wallets in the belief that the good law enforcement does in tracking down the bad actors outweighs the risk of good actors information falling into the bad actors hands.

From past experience this is a bad thesis. Information security both in the private and public sectors has not been absolute. As a result it is a matter of when not if some information contained in the BSA report databases gets stolen. When that happens there is a real risk that there will be an increase in crime in excess of the crimes prevented or prosecuted by creating the initial reporting requirement. For those unlucky CVC users that do suffer losses their losses will be absolute.

Final Summary

FinCEN does important work identifying financial crimes, disrupting terrorism, and tracking illicit flows of money. There is no denying that law enforcement helps keep our country safe. These are vital functions of government and the people who carry out these tasks are heroes. They have a significant need for information in order to identify and prosecute criminals. However their needs are not the only ones. Average Americans need tools to keep their property and their person safe. Americans of all backgrounds need the ability to fully participate in the financial system.

The proposed rules expanding BSA reporting to CVC go too far in their discrimination against CVC users by subjecting them to extraordinary reporting requirement that no other monetary instrument is subject too. It discriminates against individual users that are acting in good faith in attempting to protect CVC assets and it creates barriers against smaller dollar CVC users by imposing costly an onerous rules on the MSBs that will be tasked to implement them.

The overall net result of these rules is not one that will benefit our country. It will curtain use of CVC amongst disadvantaged communities, reduce CVC and payment innovation, and drive large users and organizations to other countries. In short these rules sacrifice long term economic prosperity for law enforcement's short term desire for information. It is the position

of this comment that the proposed rules should be abandoned all together. If the proposed rules are not abandoned all together they should at minimum be no more burdensome than the rules imposed on other monetary instruments.