

# Open Letter to FinCEN's Proposed Amendment of the BSA

10/24/20

At the core of FinCEN's proposal, having gathered opinions from the FBI, DEA, IRS, USSS and others, is lowering the threshold for the Travel Rule and Recordkeeping Rule to a \$250 threshold while simultaneously classifying some crypto currencies as a Convertible Virtual Currency ("CVC") with legal tender status.

The Agencies are proposing to **lower the threshold under the Recordkeeping Rule**, and FinCEN is proposing to **lower the threshold under the Travel Rule, to \$250** for funds transfers and transmittals of funds **that begin or end outside the United States.**

*FINCEN-2020-0002 ; RIN 1506-AB41 page 8*

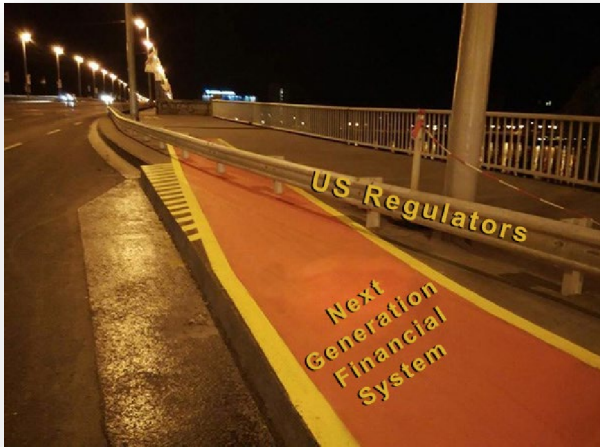
The requirement that "Funds Begin or end outside the United States" is in the title and repeated multiple times as the stated goal of this proposal. Yet several questions posed by FinCEN suggest the ultimate goal is to force regulated institutions to fund and maintain a ubiquitous financial surveillance network with real-time access reaching all the way down to local law enforcement for eventually - all transactions foreign and domestic.

This poses tremendous security questions in light of the recent FinCEN leak. It poses tremendous privacy concerns which were completely ignored by FinCEN and the Agencies. In fact, the word "privacy" is found exactly zero times in FinCEN's 14,685 word, 51-page document.

They pay lip service to financial inclusion, mentioned only one time, solely in context of enforcement and quite ironically, in quotes.

These burdensome requirements, come at a time when innovations by the small players, disproportionately affected by the proposed changes, are critical to US

maintaining a prominent position within the global financial system. A lack of regulatory clarity will persist despite this proposed rule change as I'll explain.



Inaction on behalf of the Federal Reserve has caused the United States to fall far behind their peers. Faster payment systems and CBDCs are being rolled out around the world, yet the US is still years away, with no signs of correcting this shortfall, despite available solutions.

It's gotten to the point where Fintech companies like Ripple are actively making plans to leave the US for a country taking a friendly regulatory approach like the United Kingdom, Switzerland, Singapore, Japan and others. Meanwhile in the US, Regulator's don't even seem to understand, they're the problem. This was made abundantly clear to SEC Commissioner Jay Clayton in January when he sat down with Glenn Hutchins and Gary Cohen for a talk titled:

[The State of Our Securities Markets: Current Global Macroeconomic Trends Affects Our Capital Markets](https://www.youtube.com/watch?v=IBJl8HFg_LY)  
[https://www.youtube.com/watch?v=IBJl8HFg\\_LY](https://www.youtube.com/watch?v=IBJl8HFg_LY)

The global financial system's framework, which the US will ultimately be forced to adopt, will come from Asia, because US regulators and the Agencies behind this report have failed, and continue to fail, the US financial sector.

While FinCEN shares a series of its best war stories, it fails to show the true impact and unintended consequences of its proposal on regulated Money Services Businesses ("MSBs"), the American people, their privacy, US Markets, the dominance of the US Financial system globally, and the dominance of the US dollar.

Having read every response submitted to the Federal Register related to the Consumer Financial Protection Bureau's proposed changes to the "[Remittance](#)

[Transfers Under the Electronic Fund Transfer Act \(Regulation E\)](#)”, these rule changes are likely to put some of these smaller MSBs out of business.

MSBs, small banks and credit unions that don’t have the significant capital investment required to implement compliance solutions, and don’t get free bailout money from the Federal Reserve, will be forced to shut down.

This will further consolidate and weaken the Financial sector, at a time when it should be expanding to keep pace with financial innovations happening in China, U.K., Singapore, Japan and elsewhere.

FinCEN’s analysis of the impact, focuses only on averages which look, well, very average. But Financial Institutions (“FIs”) see it differently:

At the same time, other **financial institutions expressed concern** that imposing information collection requirements (especially for smaller-value transmittals) could **increase regulatory compliance costs** by mandating the use of new technologies and processes to collect the information, and that these costs could be **passed on to consumers**. *FINCEN-2020-0002 ; RIN 1506-AB41 page 15*

These are of course the larger institutions with the capacity to interact with regulators, a resource intensive activity. Nowhere does FinCEN mention how many of the 23,234 financial institutions this may put out of business.

Instead the proposal focuses on the number of additional hours while admitting they have no idea what a compliance solution may cost,

Compliance costs for entities that would be affected by these regulations are generally, reporting, recordkeeping, and information technology implementation and maintenance costs. **Data are not readily available to determine the costs specific to small entities** and the Agencies invite comments about compliance costs, especially those affecting small entities. *FINCEN-2020-0002 ; RIN 1506-AB41 page 32*

While initially assuring us, 18 pages prior, the impact will be minimal:

**The Agencies believe that the effect** of lowering the \$3,000 threshold on financial institutions and on the cost and efficiency of the payments system **is likely to be low**. *FINCEN-2020-0002 ; RIN 1506-AB41*

*page 14*

These changes Weaken America's FIs by raising the barrier to entry, likely by millions of dollars, thereby reducing innovation-driving competition, which serves to further weaken America's position in a global race it's quite frankly, already lost.

Instead of strengthening America's financial system by working with FIs to reach regulatory clarity as other countries have done successfully, the tact taken continues to be one of regulatory enforcement that continually expresses a narrative of increased surveillance and control while offering conflicting viewpoints on digital assets, a problem that persists today.

For example, FinCEN points to a 1995 statement saying a decreased threshold may be required; implying it's a justification for the rule change:

**In the 1995** rulemaking implementing the Travel Rule, **the Treasury noted that it would monitor the effectiveness** of financial institutions' suspicious transaction reporting protocols **to determine whether potentially illicit transactions below the \$3,000 threshold were being reported** (and thus **whether it might be unnecessary, from a law enforcement perspective, to lower the threshold**). *FINCEN-2020-0002 ; RIN 1506-AB41 page 10*

There is no end to these government agencies' desire to end privacy by surveilling, recording and archiving the interactions of every individual. In the same document the agencies are laying the foundation to reference, "eliminating altogether" the threshold as a next step:

"While not the official comment of each such agency, **the agents and prosecutors** specializing in money laundering cases and who routinely use wire transfer information **supported lowering or eliminating altogether** the reporting threshold to disrupt illegal

activity and increase its cost to the perpetrators.” FINCEN-2020-0002 ; RIN

1506-AB41 page 12

FinCEN recommends eventually giving real-time access to transaction data for government agencies without a warrant or even reasonable suspicion.

This is setting itself up to be the NSA surveilling innocent Americans all over again, but tracking money instead of Internet data.

Building FinCEN’s surveillance network in this new paradigm is the foundational for the dystopian societies that Huxley and Orwell warned us about. Your children will grow up in this world too.

Worse, FinCEN and the Agencies comments around cryptocurrency are reactionary and fail to grasp the magnitude of change underway. The Internet of Value (“IOV”), (think sending packets of money over the internet instead of data), will one day replace large portions of the existing financial system, and Decentralized Finance (“DeFi”) will do it without a trusted 3<sup>rd</sup> party, often entirely opaque to law enforcement.

Within a decade the IOV will bring billions of transactions moving pennies over interconnected, interoperable networks, some of which, completely private and decentralized. At some point in the very near future FinCEN and the Agencies will have to rethink their enforcement strategies, as this proposal will hasten adoption of that new paradigm.

The Money Laundering and Asset Recovery Division at the Department of Justice (“MLARS”), rightly point out that criminals will change their behavior in order to stay under the reporting requirements:

“MLARS identified two potential concerns – first, that some **criminals would structure transactions to evade the lower threshold**, and second, **if such structuring occurred, those smaller dollar transactions would be difficult to distinguish** from legitimate

wire transfers.” FINCEN-2020-0002 ; RIN 1506-AB41 page 12

So not only are the targeted transactions likely to be lost in the noise due to this change, this response ignores the elephant in the room - the advent of the Decentralized Exchange (“DEX”). I’ll explain why DeFi renders the measures proposed by FinCEN mostly useless, later in the document.

As mentioned, FinCEN plans to create a real time database accessible to all of the aforementioned government agencies even reaching out as far as local law enforcement.

They make no mention of any privacy safeguards or measures taken to ensure access to this data is not abused.

“The **FATF recommends** that “**basic information**” concerning the originator and beneficiary of wire transfers **be immediately available to appropriate government authorities, including law enforcement and financial intelligence units**, as well as to financial institutions participating in the transaction.” *FINCEN-2020-0002 ; RIN 1506-*

*AB41 page 13:*

Given NSA employees and contractors were caught using NSA systems to spy on former partners and passing around nude photos acquired from targets’ phones, this is a more than valid concern.

This recommendation comes from an organization that just over one month ago had an unprecedented breach of the public trust when 17 years of selected Suspicious Activity Reports (“SARs”) representing 2 trillion dollars in transactions were leaked to the public.

September 23, 2020

## Leaked FinCEN files expose poor data security

Larry Jaffee



Leaked FinCEN documents that cite JPMorgan Chase and other financial institutions as processing dirty money may have come from a whistleblower or insider.

Leaked documents, dubbed the “FinCEN Files,” describe global money laundering of \$2 trillion processed by many of the world’s biggest banks between 2000 and 2017. The reveal illuminates the struggle for the financial industry and government to provide ironclad data protection.

“This sensational and unprecedented leak clearly demonstrates a wide spectrum of data protection weaknesses in the governmental sector, affecting even the most developed Western countries,” Ilia Kolochenko, founder and CEO of ImmuniWeb, said of the files.

“From a cybersecurity standpoint, we may expect a growing lack of trust to governmental agencies, which on one side have quasi-unlimited access to the most sensitive data of the largest organizations, while cannot duly safeguard this data on the other side,” he said.

By FinCEN’s own admission, their leak:

“can impact the national security of the United States, compromise law enforcement investigations, and threaten the safety and security of the institutions and individuals who file such reports.”

*FinCEN September 01, 2020 Statement*

Now FinCEN would have us reward this unprecedented failure with increased powers, access to increased volumes of sensitive data, and the capability to real time monitor all international transactions over \$250 while sharing this data with virtually anyone who wants it, including local police departments.

The lack of any concern or even comment about this real time monitoring system's potential for abuse is appalling. I hope someone in the decision-making process is asking the questions:

- Why should FinCEN be trusted?
- Why is failure being rewarded with greater responsibility?
- How can FinCEN ensure the safety and security of this data?
- What are the security implications of: A hacked feed to hide transactions; Data leaked to the public; Counter surveillance by an adversary; A compromised employee.

There's no mention of any of these issues in this proposal. It's like the **LARGEST MOST DAMAGING GOVERNMENT LEAK IN FINANCIAL HISTORY DIDN'T JUST HAPPEN, LAST MONTH.**

Are Americans due an explanation of how this happened and what safeguards have been put in place to ensure this never happens again?

Or are we being told to blindly trust FinCEN's transparency black hole?

The documents in the FinCEN files cover about \$2tn of transactions and they are only a tiny proportion of the SARs submitted over the period. <https://www.bbc.com/news/uk-54226107>

Outlined in these documents are trillions of dollars laundered through US and Foreign banks who failed to stop the money from moving. Most of these crimes haven't been prosecuted, but today, FinCEN is here to tell us \$250 transactions, are the problem.



## Decentralized Finance Implications

---

The 2015 National Terrorism Finance Risk Assessment noted:

**“terrorist financiers and facilitators are creative and will seek to exploit vulnerabilities** in the financial system to further their unlawful aims, **including**, as the above analysis indicates, through **the use of low-dollar transactions.”** *FINCEN-2020-0002 ; RIN 1506-AB41 page 9-*

*10*

FinCEN and the Agencies are highlighting their targets ability to adapt to regulations and use new and innovative means to evade authorities, while shoehorning the public into thinking this means low value transactions, transmitted via regulated FIs are the problem.

The FATF recommends that countries minimize this and other thresholds to the extent practicable, after taking into account the risk of “driving transactions underground” and the “importance of financial inclusion.” *FINCEN-2020-0002 ; RIN 1506-AB41 page 14*

They acknowledge the risk of losing visibility while simultaneously increasing financial exclusion. These transactions are far more likely to move to a privacy focused cryptocurrency-based solution that completely sidesteps KYC/AML using a DEX or series of DEXs.

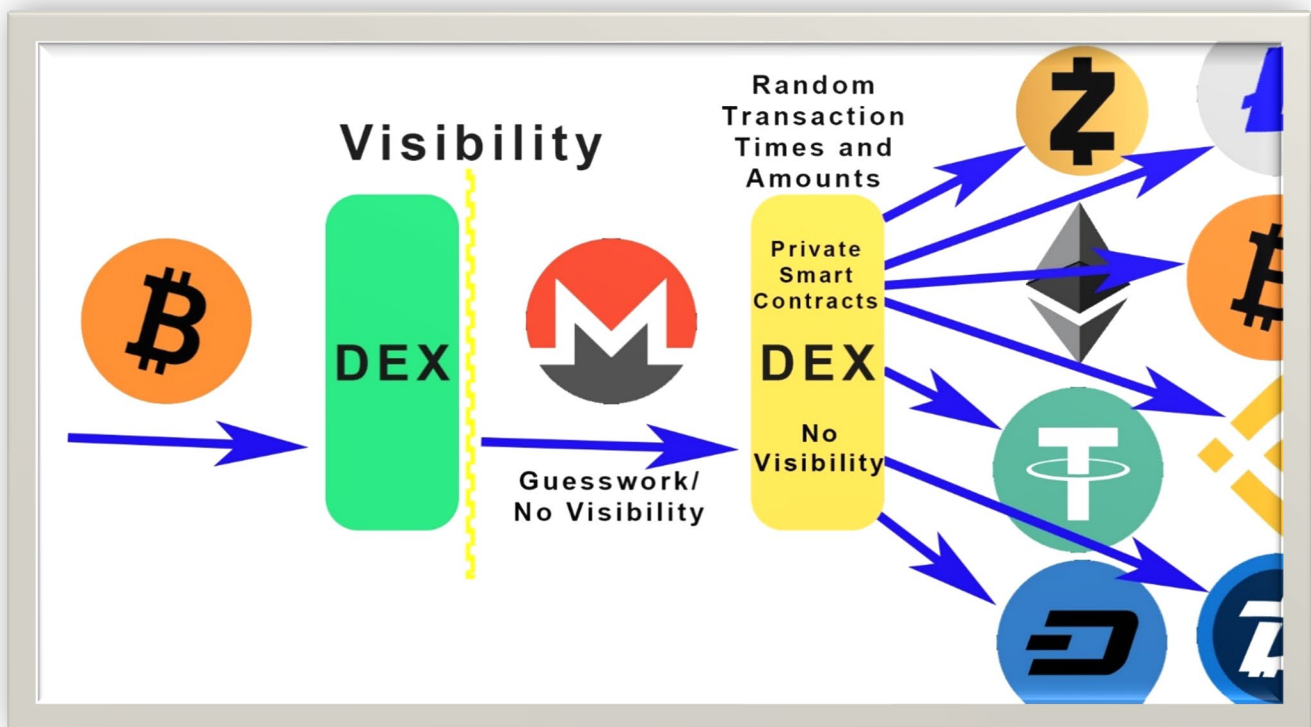
Given the IRS and Homeland Security both have bounties to deanonymize Monero transactions, it's safe to say, FinCEN and the Agencies don't have reliable visibility that provides a verifiable chain of custody.

When transactions move to the Monero blockchain they exist in a dark pool largely invisible to authorities until a trade into a crypto with a public blockchain can sometimes be inferred based on transaction characteristics.

A Decentralized Exchange is a smart contract that runs on the decentralized blockchain (Ethereum currently the most popular) that allows users to perform more advanced financial transactions.

Currently, capabilities allow a DEX to swap ERC-20 tokens on the Ethereum Network anonymously avoiding KYC/AML regulations. The Agencies could no more shut down a DEX than they could shut down the internet. There's no central party to attack, and any user can create an interface to connect to the smart contract on the blockchain to execute it.

What's currently being built and rolling out in the coming weeks are cross chain swaps. The ability to use a DEX to exchange say, Bitcoin to Monero, without KYC/AML or a 3<sup>rd</sup> party intermediary because it's enforced and executed by the decentralized blockchain.



The capability will also exist to plug a DEX into a network like Overledger or Interledger where a million-dollar transaction can be broken up into hundreds of millions of micro-payments (among billions) moving fractions of a cent out of any asset into any other asset on the network another DEX or regulated exchange is willing to offer.

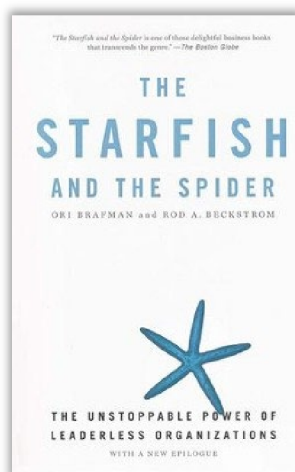
Illicit funds can be dispersed from a private coin, into 50 different wallets spread across 20 different blockchains, stable coins, tokenized assets/commodities/stocks, or wrapped assets. The transfers can be

randomized for time and dollar values, they can be run through multiple hops, decreasing risk, but increasing laundering costs.

When anyone can launder through multiple assets and end up with a privacy coin or a washed stable coin spendable digitally – why would anyone use the regulated system? When you start monitoring \$250 transactions on the regulated network, why wouldn't they start using this?

FinCEN, the Agencies, and the Federal Reserve have failed to understand the lessons offered by the digital music evolution. It started with Napster, which had some design weaknesses that, once it grew to sufficient size, caught the attention of the music industry and was shut down.

The innovative, anti-fragile idea was exchanging data in a peer-to-peer network. When the centralized attempt was stopped, a decentralized version was born. Actually, several were born including Kazaa, Limewire, e-mule, e-donkey, all evolutions that made minor improvements until BitTorrent was released. It was such a paradigm shift; it was quickly adopted and is still used today for both legal and illegal purposes.



This predictable outcome is explained in Ori Brafman and Rod A. Beckstrom's book, The Starfish and the Spider.

Decentralized networks are like starfish. You attack them and cut off a leg and two starfish grow back, leaving you with twice the problems.

Crypto works the same way. The more you attack it, the more anti-fragile and resilient against attack the network evolves to become.

The more you attack privacy coins and eventually private smart contracts, the more they will adapt and become resilient to your attacks.

The music industry fought the new paradigm for over a year before realizing the opportunity at hand. Today the music industry makes more from streaming music than selling CDs.

Music sharing still exists on the torrent networks, but think of all the ways to get music today. You can buy physical or digital, you can stream or watch free on Youtube (w/commercials).

By opening up their business models to this new paradigm, they managed to create a very healthy business with new revenue streams while minimizing unauthorized sharing. They achieved this by making the



regulated market easier to use and access than the black/gray market.

Today FinCEN and the Agencies are making this same mistake. This proposal represents yet another attempt to fight the new paradigm instead of embracing it and making as easy as possible for the regulated market to incorporate the advantages.

It won't be long before the first darknet marketplace moves to DeFi.

It will eliminate exit scams by locking escrow funds in private smart contracts. Users can opt to insure shipments, and administrators will be decentralized groups of anonymous oracles handling disputes.

Instead of taking the “*regulation through enforcement*” approach, Regulators should be pulling all the relevant agencies together with a large cross section of FIs, and working with Fintechs in the space to create a regulatory framework and definition set that's ubiquitous across all agencies.

Look at Trump's Executive Order 13827:

**foreign governments**—including Iran, Venezuela, and Russia—**have created or expressed interest in creating digital currencies** that could be **used to engage in sanctions evasion**. For example, the Venezuelan government developed a state-backed digital currency called the “petro,” which the government publicly indicated was designed for the purpose of evading U.S sanctions. **The President** subsequently **issued Executive Order 13827, prohibiting any U.S. persons from involvement in the petro digital currency**. *FINCEN-2020-0002 ; RIN 1506-AB41 page 19-20*

How is that even relevant in a DeFi paradigm arriving in a matter of months? Enforcement approaches like this proposal and this executive order only serve to breath life into the expansion of DeFi capabilities by increasing demand.

This is yet another siloed approach by a subset of agencies. This proposal suggests applying legal tender status to some digital assets and fails to provide regulatory certainty or clarity.

In the process it pushes criminals to adopt DeFi while preventing the regulated space from providing solutions which allow some visibility vs. the blackhole that DeFi can represent.

**Information available** to the Agencies **indicates that malign actors are using smaller-value cross-border wire transfers** to facilitate or commit terrorist financing, narcotics trafficking, and other illicit activity, **and that increased recordkeeping and reporting concerning these transactions would be valuable to law enforcement and national security** authorities. *FINCEN-2020-0002 ; RIN*

*1506-AB41 page 8*

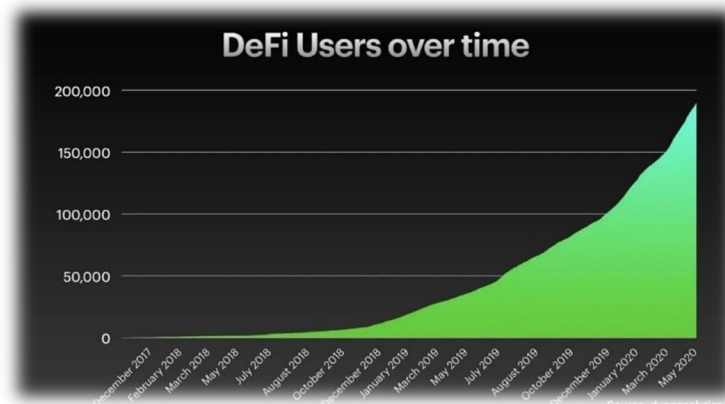
I’m sure most police departments would agree that a police state would be ideal for policing. The people living under the systems of the complete surveillance end-game this represents however, would disagree.

Generally, CVCs can be exchanged instantaneously anywhere in the world through peer-to-peer payment systems (a distributed ledger) that allow any two parties to transact directly with each other

without the need for an intermediary financial institution. However, **in practice, many persons hold and transmit CVC using a third-party financial institution such as a “hosted wallet” or an exchange.**

*FINCEN-2020-0002 ; RIN 1506-AB41 page 18*

FinCEN acknowledges that most transactions happen today on an exchange while failing to note the DeFi elephant in the room is on an exponential growth curve:



FinCEN goes on to point out that CVC transactions should be treated as cash or the equivalent legal term:

To mitigate illicit finance risks posed by CVC, the **FATF has advised that countries should** consider so-called virtual assets as “property,” “proceeds,” “funds,” “funds or other assets,” or other “corresponding value” and, consequently, should **apply relevant FATF antimoney laundering/counter-terrorist-financing measures to virtual assets.** *FINCEN-2020-0002 ; RIN 1506-AB41 page 19*

Of course, the lack of regulatory clarity and conflicting viewpoints between agencies is still a problem for FIs as FinCEN acknowledges:

However, FinCEN understands **that at least one industry group has asserted that the Recordkeeping and Travel Rules do not apply** to transactions involving CVC, **in part because the group asserts that CVC is not “money” as defined by the rules.** *FINCEN-2020-0002 ; RIN 1506-*

*AB41 page 19*

According to whose rules? That's the problem here in a nutshell. FinCEN is now calling it legal tender. How does the SEC classify Cryptocurrency? In today's environment, the agency that's correct, is the one taking enforcement action against you. That's how US regulators have strangled the financial sector at a critical time in history.

Every approach to solve this problem has been a siloed approach, because agencies are inflexible and bound by a regulatory framework that's no longer applicable to the new paradigm.

The **thresholds would be lowered from \$3,000 to \$250, but only with respect to funds transfers and transmittals of funds that begin or end outside the United States.** As set forth in the proposed revised sections below, a funds transfer or transmittal of **funds would be considered to begin or end outside the United States if the financial institution knows or has reason to know that the transmitter, transmitter's financial institution, recipient, or recipient's financial institution is located in, is ordinarily resident in, or is organized under the laws of a jurisdiction other than the United States** or a jurisdiction within the United States. *FINCEN-2020-*

*0002 ; RIN 1506-AB41 page 21*

So, we're to treat digital assets as Cash equivalents which will be subject to KYC/AML requirements based on KYC information submitted. But again, FinCEN and the Agencies remind is that this **only** applies to international transactions and **not domestic**. Only there's a problem with that narrative.

Clinton Donnelly, a US Tax Expert, points out **the IRS position is that ALL exchange transactions are to be considered anonymous and it therefore must be assumed a foreign transaction requiring KYC/AML!**

The IRS requires a Form 8938 be filed for KYC/AML reasons under the IRS tax code 26 U.S. Code § 6038D - Information with respect to foreign financial assets. The IRS uses an automated business intelligence system to identify crypto traders and fine them \$10,000 for not filing Form 8938.

Clinton Donnelly Interview: [https://youtu.be/rx6Owz5l\\_EE?t=556](https://youtu.be/rx6Owz5l_EE?t=556)

Again, this proposal makes it abundantly clear that FinCEN and the Agencies, which includes the IRS, do not intend to use this for domestic transactions. There is also no mention of all Crypto/CVC transactions being classified as international transactions subject to this rule.

This means one of two things:

- A) The IRS has incompetently endorsed a policy in this proposal related to KYC/AML for crypto transactions that directly conflicts, with the IRS Policy (and law) on KYC/AML for crypto transactions.

Or;

- B) This proposal is intended as a trojan horse, and the public is being intentionally misled by FinCEN and the IRS in order to accomplish two objectives:
  - a. The ability for the IRS to leverage US regulated exchanges, at any time, by pointing to this law and requiring exchanges give the IRS access to all crypto transactions over \$250. Potentially also giving them a real-time feed as FinCEN recommends.
  - b. Thereby also forcing exchanges to perform KYC/AML for any customer transacting over \$250.

If it's the former, then one of the two policies must be corrected unless we're throwing the Equal Protection clause of the 14<sup>th</sup> amendment out the window.

It stands as yet another example that the confusing and contradictory framework has gotten so bad, it's now happening within the agencies themselves! It represents a monumental failure of this effort by FinCEN and the Agencies.

If it's the latter, this represents a serious breach of the public trust. The public deserves answers and clarifications on this issue. Given other questions posed by FinCEN and the Agencies, total surveillance is clearly the implied long-term goal.

**What would be the impact on the burden if the proposed threshold change were extended to all transactions, including domestic transactions?** *FINCEN-2020-0002 ; RIN 1506-AB41 page 23*



Are FinCEN and the Agencies intentionally attempting to mislead the public?

This proposed rule would define “money” in 31 CFR 1010.100(II) and (eee) to make explicitly clear that both payment orders and transmittal orders include any instruction by the sender to transmit CVC or any digital asset having legal tender status to a recipient.<sup>46</sup> The proposed rule would therefore supersede the UCC’s definition of “money”. *FINCEN-2020-0002 ; RIN 1506-AB41 page 20*

Defining CVCs and digital assets as money is a step in the right direction, but not when the IRS is going to continue treating it as an equity subject to capital gains.

FinCEN and the IRS tell us it’s money in this proposal, but in fact, here are the IRS’s simple, 6 step process for reporting the purchase of a cup of coffee with crypto, which you now define as money:

Action: Buy a coffee with Monero (XMR)

Details: 0.05 XMR sent from your private wallet to a shop's XMR wallet to purchase a coffee

Accounting steps:

**1) Calculate your cost basis of XMR sent**

1a) Using First-In-First-Out (FIFO) accounting, identify the oldest unspent XMR in your records of all cryptocurrency trades that you've ever made

1b) Calculate the USD value of these oldest unspent coins at the time of original purchase. If the XMR was purchased with BTC, go to a lookup table of averaged exchange data for USD/BTC price at the time of XMR purchase and convert the BTC purchase price to USD.

1c) Be sure to include a calculation of cost basis for the XMR transaction fee as there will be capital gains on this as well.

1d) Repeat this process if XMR used in purchase can be tracked to multiple purchase transactions according to FIFO designation

1e) Update your FIFO records to reflect that these oldest XMR are now "spent"

**2) Calculate the USD value of XMR and XMR fees at the time of the transaction**

2a) Using a lookup table, calculate the average exchange price for BTC/USD at the time of purchase

2b) Using a lookup table, calculate the average exchange rate for XMR/BTC at the time of purchase

2c) Using exchange rates from Steps 2a and 2b, multiply (XMR + XMR transaction fee) by BTC/XMR ratio from 2b, then multiply by USD/BTC rate to calculate the USD value of XMR and XMR fees used in the current transaction

**3) Calculate Gain/Loss of XMR and XMR fees**

3a) Subtract the cost basis determined in Step 1 from the USD value determined in Step 2 for USD value of XMR plus XMR transaction fees

3b) Identify whether the oldest unspent coins from Step 1a were purchased more than a year ago

3c) If coins older than a year, record the Gains/Losses from Step 3a as a long-term capital gain/loss

3d) If coins held less than a year, record the Gains/Losses from Step 3a as a short-term capital gain/loss

**4) Pay taxes for 2019 tax year**

4a) File Form 1040 to the IRS for tax year 2019 which includes the Gains/Losses calculated in Step 3 as long-term gains recorded on Line 13 or as short-term gains recorded on Line 14 in the form. Include all cost basis, timing, and price details in an attached 1099-K of the XMR transactions used to purchase the coffee. This could include multiple line items if multiple purchase transactions were identified through FIFO as being the source of unspent coins used during the coffee purchase transaction.

4b) Calculate federal taxes owed by determining your applicable capital gains tax rate for 2019 and multiplying by your long-term capital gains from the transaction. Calculate short-term gains according to your applicable short-term rate. Depending on your tax bracket, these may be as high as 18% and 38% of gains, respectively.

4c) Calculate state taxes owed (varies drastically from state to state). Determine tax liability from both long-term and short-term gains or losses.

**5) If a gain was determined in Step 4a and tax liability is owed, then pay federal and state tax authorities the owed tax liability.**

**6) Make four estimated tax payments in 2020. If you expect to continue buying coffee in 2020, then file a federal Form 1040-ES and make quarterly estimated payments to the US Treasury for the approximate annual gains to be made in the underlying cryptocurrency asset being used in the expected purchases. A defensible position is to take the tax liability calculated in Step 4b and divide these totals by 4 to determine how big of quarterly federal tax payments to make. Depending on your state of residence, you may be required to make quarterly payments to your state taxing authority as a function of 2019 gains calculated in Step 4c.**

*Source:* [https://www.reddit.com/r/CryptoCurrency/comments/cj0m0h/tax\\_ramifications\\_of\\_buying\\_coffee\\_with/](https://www.reddit.com/r/CryptoCurrency/comments/cj0m0h/tax_ramifications_of_buying_coffee_with/)

How is this mess eliminated as part of the proposal given a Crypto is now classified as money, or have you simply added to the complexity of the conflicting overlapping definitions from the various regulatory agencies which have paralyzed the US financial sector while progress is being made elsewhere?

Is anyone in the government responsible and accountable to taxpayers trying to sort this nonsense out? From here it looks as if the Agencies just don't care about the conflicts and only focus on their little fiefdom leaving most American businesses and consumers lost at sea.

**The Treasury, including FinCEN, has closely monitored illicit finance risks posed by CVCs.** The Agencies note that malign actors have used CVCs to facilitate international terrorist financing, weapons proliferation, sanctions evasion, and transnational money

laundering, as well as to buy and sell controlled substances, stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms, and toxic chemicals. *FINCEN-2020-0002 ; RIN 1506-AB41 page 19*

And yet no mention of the impact DeFi or DEXs using private smart contracts, the advent of stable coins, as well as wrapping of existing public coins for trustless cross chain swaps? How was this missed?

Everything listed above is available on most darknet markets. Surely the Agencies are aware this will migrate to a DEX with even fewer weaknesses to exploit, far less visibility, and no admins running it to flip as informants?

“The **following two sections lay out**, respectively, (A) the **potential benefits to national security and law enforcement** from reducing the Recordkeeping Rule and Travel Rule thresholds for funds transfers and transmittals of funds that begin or end outside the United States, and (B) **the potential effect these new requirements would have on the cost and efficiency of the payments system.**”

*FINCEN-2020-0002 ; RIN 1506-AB41 page 8*

This proposal does a risk assessment based on the above to factors by first creating a bubble, where the proposed changes can only impact finances related to compliance costs.

**FinCEN believes the primary cost of complying with the proposed rule is captured in its Paperwork Reduction Act (44 U.S.C. 3507(d)) (“PRA”) burden estimates described in detail below, which amount to 3,315,844 hours. . . . Therefore a reasonable minimum estimate for the burden of administering the proposed rule is approximately \$79.58 million annually (3,315,844 hours multiplied by \$24 per hour). However, the PRA burden does not include certain costs, such as information technology implementation costs solely resulting from the need to comply with this proposed rule.** *FINCEN-*

*2020-0002 ; RIN 1506-AB41 page 25*

Yet they have failed to estimate the cost to acquire and maintain a compliance system. On the national security side, consideration is given solely to terrorist attacks.

it is difficult to quantify the contribution of a particular rule to a reduction in the risk of a terrorist attack. However, even if the proposed rule produced very small reductions in the probability of a major terrorist attack, the benefits would exceed the costs. *FINCEN-*

*2020-0002 ; RIN 1506-AB41 page 24*

This analysis is beyond flawed, as it fails to acknowledge the unintended consequences these changes will produce. What is the threat to national security of the dollar losing global reserve status? What is the threat to national security and the prosperity of the American people if the US financial markets lose dominance to Asia?

FinCEN estimates a terror attack in the tens of billions, yet the risks are in the hundreds of billions for decades to come.

For instance, if the proposed rule reduced by 0.26 percent the annual probability of a major terrorist attack with an economic impact of \$30 billion, the benefits would be greater than the PRA burden costs described above. *FINCEN-2020-0002 ; RIN 1506-AB41 page 26*

And it's happening right now. Below is a tweet from the CEO of Ripple, a fintech company at the center of evolving the global financial system with a CVC bridge asset XRP.

I'm sure FinCEN will recall the enforcement action it took against Ripple Labs in May of 2015 and fined them \$450,000 over this very issue. Ever since Ripple has been working with, begging and pleading regulators to provide regulatory clarity for their industry.

Yet here we are almost 5 years later and as a government entity you continue to provide conflicting positions as pointed out by the CEO of Ripple on October 8th:



They've been trying to work with regulators for years now, and the lack of clarity is causing stagnation in the evolution of our financial system at the cost of US dominance, and Ripple, a soon to be trillion-dollar payments company at the center of this change, is making plans to leave.

What's that impact on the US economy? On national security? On US dominance in the global financial system?

<https://twitter.com/bgarlinghouse/status/1314279492618256387>

Banks and FI's are terrified of running afoul of the law, negating any savings because for 5 years you have failed them. With this proposal, you fail them yet again. Yet according to FinCEN and the regulatory agencies consulted in this report:

**The Agencies are unaware of any Federal rules that duplicate, overlap with, or conflict with the proposed changes to the Recordkeeping and Travel Rules** *FINCEN-2020-0002 ; RIN 1506-AB41 page 33*

FinCEN and the Agencies are wearing blinders to only see the narrowly defined impact on the industry, while failing to see the unintended consequences that are orders of magnitude greater.

To what extent would the burden of the proposed rule be reduced if the Agencies issued specific guidance about appropriate forms of identification to be used in conjunction with identity verification, including in regards to whether there are circumstances in which verification may be done remotely and what documents are acceptable as proof? *FINCEN-2020-0002 ; RIN 1506-AB41 page 23*

Have the Agencies considered the impact that various Open ID projects could have on these regulations? It appears the government is once again stuck in the existing paradigm and making no effort to look at what's on the horizon.

Reducing the threshold to trigger KYC/AML to include everyday transaction amounts while intending to eliminate the threshold all together one day, creates another dangerous situation for privacy. With IOV streaming payments, this will tie an individual's identity to their streaming payments.

FinCEN's recommended system would give wide swaths of government agents the ability to monitor the websites and services being used, how much time is spent on each and when they were used. Just like with DeFi, there are IOV implementations that protect privacy by obscuring this information.

Regardless, this is setting up the foundation for a driver's license to use the web. This proposal is building the framework to require everyone to first identify to the government then engage in commerce and use modern services available on the internet in order to survive.

This gives the government the ability to create a "no fly list" but for the financial system. Thus, granting the state the power to unplug individuals from the ability to engage in commerce. This recommended system will be ripe for abuse and a civil rights lawsuit waiting to happen.

What mechanisms have persons that engage in CVC transactions developed to comply with the Recordkeeping Rule and Travel Rule

and what is the impact of adopting these solutions on the CVC industry, including on other BSA compliance efforts? *FINCEN-2020-0002*  
; RIN 1506-AB41 page 24

Ripple has a line of credit product which uses XRP to position capital around the world at a fraction of today's cost in just days vs. months.

[Fund Instant Cross-Border Payments With a Line of Credit From RippleNet](#), describes the ability to quickly deploy capital in foreign markets. Customers can also use Ripplenet and the digital asset XRP to facilitate cross border payments at a fraction of current costs.

Ripplenet integrates automated KYC/AML checks as part of its pre-transaction messaging. On the XRP ledger, travel rule information can be encrypted between the end parties, permanently stored on the public blockchain and moves with the funds. It's fully compliant, easily adaptable, and FI's would love to use it.

Unfortunately, conflicting regulatory positions have FIs sitting on the sidelines. As I'm wrapping up this document Brad is tweeting again on this very issue:



**Brad Garlinghouse** ✓  
@bgarlinghouse

1/ UK's FCA and Singapore's MAS have been leaders for years in providing clarity on using/trading assets - no surprise that both countries have traditional FIs leaning into using this technology. DBS' (pre)announcement today is a prime example. (1/2)



**Ryan Browne** ✓ @Ryan\_Browne\_ · Oct 23

"The U.S. is out of sync with other G20 markets"

I spoke with Ripple CEO @bgarlinghouse about the crypto company's threat to leave the US

He says he was in London recently and that the UK's FCA offered "clarity that XRP is not a security" [cnbc.com/2020/10/23/cry...](https://www.cnbc.com/2020/10/23/cry...)

[Show this thread](#)

2:21 PM · Oct 27, 2020 · Twitter Web App



**Brad Garlinghouse** ✓  
@bgarlinghouse

Replying to @bgarlinghouse

2/ Some have suggested Ripple is "fleeing" the US, let me unequivocally say this is absolutely not the case. We're a proud US-based company, and would like to stay here but a lack of regulatory clarity and level playing field is forcing us to evaluate other jurisdictions. (2/2)

2:21 PM · Oct 27, 2020 · Twitter Web App

While facing multiple threats from all sides to the Dollar's global reserve status, US regulators, FinCEN, the Agencies and the SEC are failing the industry they claim to serve, and ensuring American businesses are disadvantaged for decades to come.

[Referenced CNBC Article](#)

## FinCEN Continues:

Of course, the proposed rule would not simply reduce the probability of terrorism but also would contribute to the ability of law enforcement to investigate a wide array of other priority transnational threats and financial crimes, including proliferation financing, sanctions evasion, and money laundering. *FINCEN-2020-0002* ;

*RIN 1506-AB41 page 26*



Unfortunately, the reality of that statement is that FinCEN is about to push criminals to a platform where they will lose all visibility, while increasing demand.

FinCEN suggests that it's considered all available options and tries to paint the picture that, the proposed solution, is the only option:

**FinCEN considered** the possibility of modifying the proposed rule by applying the **FATF's suggested de minimis threshold of \$1,000** to transactions that begin or end outside the United States. However, **this threshold would exclude over 88 percent of the transactions in FinCEN's dataset** of transactions **potentially linked to terrorism.**

*FINCEN-2020-0002 ; RIN 1506-AB41 page 26-27*

If I understand FinCEN's examples correctly, the vast majority of those transactions were collected voluntarily by MSBs in cooperation with FinCEN.

Suggesting they would lose access to that information going with the FATF's standard, while insisting on an Orwellian surveillance system starting at \$250 and moving to \$0 for all transactions including domestic, is presenting a Hobson's choice.

The reality is FinCEN could work WITH the industry to catch bad actors with the current regulations already in place. There's no need to create casualties in the MSB industry, limit consumer choice and competition in the marketplace, not to mention the very dangerous privacy implications.

Second, **FinCEN considered** the possibility of implementing the proposed rule with **a threshold of \$0** for transactions beginning or ending outside of the United States. FinCEN's terrorism-related transaction analysis suggests that **transactions potentially related to terrorism occur at values below the \$250** level. Although FinCEN believes that a \$0 threshold would lead to enhanced benefits in terms of capturing a larger universe of transactions, **requiring collection and verification of transaction information for low-value transactions could impose a substantial burden on small financial**

**institutions, such as small money services businesses.** *FINCEN-2020-0002*

*; RIN 1506-AB41 page 27*

This is absolutely a correct assessment. Forcing them to implement, maintain and support an automated up to date compliance system is also a substantial burden and will likely force closures and consolidation in an industry trying to move us into the digital financial system. You're about to attack the innovators truly driving change, and further restricting the evolution of US markets.

This is why the blockchain, DLT based, global financial system is being built and run in Asia. Because the organizations behind this report have literally strangled innovation in this country. The consequences of America losing significant control of the global financial system will have lasting impacts felt for generations.

This proposal misses the forest for the trees.

**Applying the requirements to all domestic transactions** would therefore capture a relatively small number of additional transactions while resulting in **significant additional recordkeeping burden** for financial institutions. FinCEN believes that, **at this time, it would therefore be appropriate to limit** the proposed rule to transactions that begin or end outside the United States. *FINCEN-2020-*

*0002 ; RIN 1506-AB41 page 27*

Find me the company determines the impact of a proposed project on their bottom line – before they've even put a budget for the project together. It doesn't happen, and yet that's exactly what FinCEN and the Agencies have done here:

Although **the Agencies believe that the proposed regulatory changes would affect a substantial number of small entities**, the Agencies also believe these changes would be **unlikely to have a significant economic impact on such entities.** *FINCEN-2020-0002 ; RIN 1506-*

*AB41 page 28-29*

On page 30, FinCEN acknowledges that this change affects primarily small banks, credit unions, and money transmitters:

based upon current data there are **5,306 banks, 5,236 credit unions, and 12,692 money transmitters** that would be **impacted by the proposed rule changes**. Based upon current data, for the purposes of the RFA, there **are at least 3,817 small Federally-regulated banks and 4,681 small credit unions**. *FINCEN-2020-0002 ; RIN*

*1506-AB41 page 30*

But concludes with its opinion that this will be a minimal change for these thousands of small companies to source and implement a compliance solution, then train staff.

**the Agencies believe** that the **changes would not have a significant economic impact on such entities** for the reasons noted below. In the first year, the Agencies expect additional expense of time and resources to read and understand the regulations and train staff and implement technological changes. *FINCEN-2020-0002 ; RIN 1506-AB41*

*page 30*

Did FinCEN conduct a poll on the last internal conference call to arrive at this conclusion or was hard data analyzed? Has FinCEN reviewed a single budgetary proposal from these thousands of firms required to implement this solution? We find out two pages later:

**Compliance costs for entities** that would be **affected** by these regulations are generally, reporting, recordkeeping, and information technology implementation and maintenance costs. Data **are not readily available to determine the costs specific to small entities** and the Agencies invite comments about compliance costs, especially those affecting small entities. *FINCEN-2020-0002 ; RIN*

*1506-AB41 page 32*

So how did the agencies involved come to the conclusion that these changes would not have an economic impact when they haven't a clue how much it will even cost to implement?

FinCEN is proposing changes that could literally force dozens of these businesses to shutter operations or face enforcement. This at a time when these are the innovators leading the way towards a new financial paradigm. This is simply unacceptable.

**As described above**, the proposed rule would also clarify the Agencies' existing interpretation that the Recordkeeping and Travel Rules apply to transactions involving a digital asset with legal tender status. The Agencies do not believe that any financial institutions currently facilitate transactions involving sovereign digital currencies. *FINCEN-2020-0002 ; RIN 1506-AB41 page 31*

A company called Ripple has over 400 banks and FIs on a product it calls Ripplenet. Every one of these 400 institutions can enable a feature to use a digital asset, XRP, to facilitate cross boarder payments.

KYC/AML checks are automated, and Travel rule information is encrypted and moves with the payment, stored on the XRPL blockchain encrypted so that either party to the transaction can decrypt and store.

When using a digital asset like XRP these institutions report saving 40-60% over existing methods. Yet only a couple dozen use it today. Why?

Because US Regulators have failed them and continue to fail them with approaches exactly like this one.

## Conclusions

---

The intent of the proposed changes is to allow FinCEN and the Agencies access to additional data for investigations. While some costs have been considered, critical items like compliance systems have not.

As outlined, the proposed changes put FinCEN and the Agencies further down the road they're already on. Meanwhile an industry begging and pleading for clarity, still won't get it.

This has absolutely dire consequences for US markets by putting the financial sector at a severe disadvantage to the other G20 countries. As

innovation happens elsewhere, the US withers under a regulatory regime trapped by the complexity of its own framework and completely unable to provide leadership on this issue.

The complete disregard for privacy and the implications for our society are extremely troubling. What FinCEN proposes working towards is a dystopian privacy nightmare, that has very serious long-term implications for our society. I highly recommend watching [Glenn Greenwald's TED talk](#) about Privacy in 2014 in light of the Snowden leaks. The parallels offer lessons and explain the dangers of a society under total surveillance.

The solution proposed comes at a significant cost to the poor who use these services for remittances. It's likely to put companies out of business. It's adding well over \$70M in additional annual costs.

Meanwhile DeFi, the giant elephant in the room FinCEN and the Agencies fail to acknowledge, renders these measures obsolete in a matter of months. It's a, cut one of the legs off the starfish approach, while thinking it solves the problem. This will breath new life into DeFi where visibility can be nearly zero.

I understand there are real threats and dangerous people that wish to harm others. I think the solution is to continue taking a partnership approach with these FIs as you have been.

I don't think it's quite dawned on you all, just how radically the financial system is transforming. I hope this document has given you new perspectives. You can go on fighting the change, which makes it grow, or you can learn from the music industry, and embrace it by making some tough choices about what's really important.

The sooner consumers are plugged into a seamlessly integrated digital financial system, the sooner you stop creating new starfish.

## To the Federal Reserve board members:

For decades now you have turned a blind eye while participating in the manipulation and outright fraud in markets. LIBOR rates were rigged costing US borrowers billions. Rating agencies were completely compromised and liar loans were running rampant.

This cost people their homes, their careers, destroyed their lives, and left many destitute and homeless. Despite widespread corruption and lawlessness, there were no serious consequences for bad actors. The banks knew as soon as Paulson and Geithner slapped them with the Systemically Important Financial Institution (“SIFI”) label, they could get away with murder, and they did.

The corruption and market rigging, much of which continues today, were common knowledge, but today, today the Federal Reserve, is here to tell us \$250 transactions are the problem.

The Fed added trillions to their books to cover for these SIFIs, and when they tried to offload that steaming pile of debt propping up the housing market since 2008, the wheels came off the cart.

Now you have trillions more keeping the stock market afloat. All the relevant metrics from employment to inflation have been manipulated beyond meaningfulness. This debt will never come off your books because Fed and government policies have turned Wallstreet into a bunch of junkies with a multi-billion dollar daily habit.

Rates can't raise without default, how negative can you go without eliminating cash (and more importantly sound money alternatives)? There are no options left but to print the dollar into the ground. When you roll out a dollar “Fuente” that's fractionally backed with gold, it poses the question:

When consumers are plugged into a digital DLT/blockchain based financial system with the ability to seamlessly move between crypto assets and fiat debt notes – they will have the ability to store their wealth in any asset they choose.

Will they choose a depreciating asset like fiat with a fractional gold backing slowly degrading into oblivion? Or will they store their wealth in a cryptographically secured and provably sound money?

What happens to demand for Fiat when wealth is stored in sound money and even merchants prefer crypto? What happens when transactions start excluding Fiat all together?

What does that do to the demand equation for a “barbarous relic” only used nowadays to pay the government their taxes? How quickly will that shorten the lifecycle between monetary debasement and price inflation?

I fail to see a path forward for the Federal Reserve given the reality that’s on our doorstep.

”I know you’re out there. I can feel you now. I know that you’re afraid. You’re afraid of us. You’re afraid of change. I don’t know the future. I didn’t come here to tell you how this is going to end. I came here to tell you how it’s going to begin. I’m going to hang up this phone, and then I’m going to show these people what you don’t want them to see. I’m going to show them a world, without you. A world without rules and controls; Without boarder and boundaries; A world where anything is possible. Where we go from there is a choice I leave to you.”

~Neo

---