Further Supplemental Comments to the Financial Crimes Enforcement Network on Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets

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

FinCEN Docket No. FINCEN-2020-0020, RIN 1506-AB47

March 15, 2021

To whom it may concern:

Coin Center is an independent nonprofit research and advocacy center focused on the public policy issues facing cryptocurrency technologies such as Bitcoin. Our mission is to build a better understanding of these technologies and to promote a regulatory climate that preserves the freedom to innovate using open blockchain technologies. We do this by producing and publishing policy research from respected academics and experts, educating policymakers and the media about blockchain technology, and by engaging in advocacy for sound public policy.

We previously filed two comment letters in this proceeding and are now filing this third letter as a supplement to address remaining issues and events that have since transpired.

The procedural and statutory deficiencies in this rulemaking, detailed in our past two comments,[1] have been ameliorated with the recent 60-day comment period extension[2] and the passage of the 2021 National Defense Authorization Act (NDAA).[3] We are especially heartened that FinCEN no longer wishes to rush this important process and has allowed the public a reasonable opportunity to consider the proposal.

Customer counterparty identification is infeasible and unacceptable for privacy reasons

The customer counterparty identification requirement in both the proposed $3,000+ recordkeeping rule,[4] as well as the proposed virtual currency transaction report remains,[5] as we described in our previous two comments, a grave threat to personal privacy,[6] Fourth

---

[1] Peter Van Valkenburgh and Jerry Brito, "Comments to the Financial Crimes Enforcement Network on Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," *Coin Center*, FinCEN Docket No. FINCEN-2020-0020, RIN 1506-AB47, December 22, 2020, https://www.coincenter.org/comments-to-the-financial-crimes-enforcement-network-on-requirements-for-certain-transactions-involving-convertible-virtualcurrency-or-digital-assets/; Peter Van Valkenburgh and Jerry Brito, "Supplemental Comments to the Financial Crimes Enforcement Network on Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," *Coin Center*, FinCEN Docket No. FINCEN-2020-0020, RIN 1506-AB47, January 7, 2021, https://www.coincenter.org/supplemental-comments-to-the-financial-crimes-enforcementnetwork-on-requirements-for-certain-transactions-involvingconvertible-virtual-currency-or-digital-assets/.

[2] "FinCEN Extends Comment Period for Rule Aimed at Closing Anti-Money Laundering Regulatory Gaps for Certain Convertible Virtual Currency and Digital Asset Transactions," Financial Crimes Enforcement Network, January 14, 2021, https://www.fincen.gov/news/news-releases/fincen-extends-comment-period-rule-aimed-closing-anti-money-laundering.

[3] National Defense Authorization Act for Fiscal Year 2021, H.R.6395, 116th Congress (2019-2020) *available at* https://www.congress.gov/bill/116th-congress/house-bill/6395/text; *and see*: Peter Van Valkenburgh and Jerry Brito, "Supplemental Comments to the Financial Crimes Enforcement Network on Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," *Coin Center*, FinCEN Docket No. FINCEN-2020-0020, RIN 1506-AB47, January 7, 2021, https://www.coincenter.org/supplemental-comments-to-the-financial-crimes-enforcementnetwork-on-requirements-for-certain-transactions-involvingconvertible-virtual-currency-or-digital-assets/ (pages 4-10 regarding statutory authority).

[4] Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets,"Notice of Proposed Rulemaking, Financial Crimes Enforcement Network of the U.S. Treasury Department,85 FR 83840-62, RIN 1506-AB47, https://www.federalregister.gov/public-inspection/2020-28437/requirements-for-certain-transactions-involving-convertible-virtual-currency-or-digital-assets, at 31.

[5] *Id*., at 66.

[6] Peter Van Valkenburgh and Jerry Brito, "Comments to the Financial Crimes Enforcement Network on Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," *Coin Center*, FinCEN Docket No. FINCEN-2020-0020, RIN 1506-AB47, December 22, 2020, https://www.coincenter.org/comments-to-the-financial-crimes-enforcement-network-on-requirements-for-certain-transactions-involving-convertible-virtualcurrency-or-digital-assets/ (pages 26-33 regarding privacy).

Amendment rights against warrantless search,[7] as well as a substantial threat to continued responsible innovation.[8] For reasons we offered in our previous comments, which we will not fully rehearse here, any final rule must not include mandatory customer counterparty identification.

Financial institutions have no consistent process by which they could reliably obtain the name and physical address of customer counterparties (irrespective of whether there is an obligation to verify the supplied identity or not[9]). Counterparties may be non-human smart contracts lacking a name and physical address rendering compliance impossible. Similarly, Financial Institutions have no business inquiring into these personal details when, as will often be the case, these counterparties are not their customers and have never agreed to any disclosure of their personal information to these institutions or to the government. Any form of counterparty recordkeeping or reporting would be a profound expansion of the already substantial warrantless surveillance regime implemented by Treasury under the Bank Secrecy Act and it would trigger constitutional challenges.

Setting the counterparty requirements aside, there is the proposed virtual currency transaction report (CTR), which we will discuss in the remainder of this comment.

Virtual currency CTRs should not be implemented at present

While CTRs are already de rigueur within the legacy payments space, we do not believe that they should be extended to virtual currency transactions at the present moment. In the recently enacted NDAA, Congress made clear that it intends for the Treasury Department to reappraise the relative value of CTRs against their costs (measured in *both* the costs of compliance for regulated financial institutions *as well as* the costs to American residents in personal privacy forgone).[10] Especially noteworthy is Congress's insistence that the $10,000 threshold for CTRs be reconsidered and potentially made inflation-adjusted.[11] When the Bank Secrecy Act (BSA) was first implemented in 1970, the nominal $10,000 threshold for CTR reporting was, in present purchasing power, equivalent to $67,418.[12] A rule that forces banks to report on innocent customer transactions whenever they are greater than a luxury automobile purchase

[7] *Ibid*., regarding the Fourth Amendment.
[8] *Id*., at 27.
[9] We note that the current proposal explicitly does not call for verification. While this may lighten the burden from a compliance standpoint it does not address the fundamental issue that there will be many occasions (as with cash withdrawals) where the reporting institution will not have any way to know the name and physical address of persons their customers are paying. Nor will it address the issue of payments to non-human CVC addresses such as smart contracts.
[10] *Supra* note 3 at Secs. 6201-16.
[11] *Id*.
[12] Calculated using U.S. Bureau of Labor Statistics CPI-U (all urban consumers) inflation calculator, accessed March 11, 2021, available at: https://www.bls.gov/data/inflation_calculator.htm.

is very different from a privacy and civil liberties standpoint than a rule that demands reports for transactions around the value of a used truck or the cost of campaigning for local office.

Furthermore, the domestic CTR requirement, which self-evidently mandates warrantless searches and seizures of American's otherwise private financial papers,[13] was narrowly found constitutional by the Supreme Court only *as applied* in the original implementing regulations. Since then, we have seen a lowering of the threshold through inflation to sweep up far more personal data, and we have seen new alternative reporting and surveillance schemes implemented, such as Suspicious Activity Reports (SARs).[14] Given that a SAR is mandatory for any transaction over $2,000 that is "relevant to a possible violation of law or regulation,"[15] it is apparent that every CTR filed without an accompanying SAR is, by definition, a report about someone who has done absolutely nothing to warrant suspicion. This standard of bulk private information collection is an affront to American's Fourth Amendment right to be secure against a search unless a judge has found specific and reasonable grounds to allow for one. The Court will have several opportunities to reconsider the constitutionality of the BSA in the coming years and has, of late, shown deep suspicions over the continued vitality of the so-called "third-party doctrine" exception to warrantless search upon which the continued constitutionality of BSA reporting is predicated.[16] In light of Congress's call for a reevaluation and the significant Constitutional issues at stake, it is imprudent for FinCEN to extend CTR requirements to CVC transactions (or, indeed, to any new class of transactions) at the present moment.

If a virtual currency CTR requirement is created, it must not be more privacy-invasive that traditional CTRs

If FinCEN remains convinced that the otherwise innocent transactions of American residents must continue to be surveilled in the context of new technologies, and therefore also insists on implementing a virtual currency transaction report, then that report should by no account demand any more private data than is already reported by traditional financial institutions in traditional CTRs.

The singular discrete data point that a traditional CTR affords regulators and law enforcement is the fact that a particular customer has moved $10,000 or more from the regulated financial

---

[13] No warrant or even subpoena is necessary for FinCEN to obtain this private information about bank customers. Banks are obligated under the Bank Secrecy Act to send these reports *sua sponte*.
[14] "Amendment to the Bank Secrecy Act Regulations; Requirement To Report Suspicious Transactions," Financial Crimes Enforcement Network, 85 FR pg. 4326, RIN 1506-AA13, February 5, 1996, https://www.fincen.gov/sites/default/files/shared/fr05fe96ra.pdf.
[15] *Id.*
[16] *See generally*: *Carpenter v. United States* (Gorsuch, N., dissenting).

system to the unregulated space of physical bearer instruments (cash and similar assets).[17] The government will not learn what an individual is planning to do with the cash and will not be able to trace subsequent movements of the cash, but the risk inherent in those unsurveiled flows has historically been addressed by the need to file a simple report marking the transition and the name of the person who initiated it: Person X has taken amount Y out of the surveilled global financial system and moved it to the the freer world of physical cash.

To genuinely create parity between that legacy transaction reporting and virtual currency transactions, FinCEN must not adopt the currently proposed virtual currency transaction report form.[18] That proposed form would require the reporting of several more very sensitive pieces of data than are found in traditional CTRs.[19] It would endanger innocent users of cryptocurrency and prejudice these innovative tools by imposing stricter and more invasive regulations upon financial institutions when they deal in these novel transaction types.

It is true that *some* CVC blockchains can afford regulators with more information than a cash transaction would. This data may or may not include a transaction ID or hash, sender and recipient addresses, evidence of future transactions beyond the initial first hop, and signature data from the transaction participants. However, *not all blockchain transactions will have this information in an available form*.[20] Mandating the specific inclusion of any of these data in a virtual currency transaction report (VCTR) would not be technology neutral: it would prejudice CVCs that have been rightly designed to limit the public revelation of private financial data (such as Zcash[21] and Monero[22]) and prejudice new transaction types on top of otherwise public chains (such as Lightning network[23] and Taproot[24]-enabled transactions on top of Bitcoin).

---

[17] A CTR can be filed with form 104 and it can be completed accurately such that it reveals on, for example, that a named customer whose identity has been validated has withdrawn $10,000 on a certain date.

[18] *Supra* note 4 at 66.

[19] "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," Financial Crimes Enforcement Network, RIN 1506-AB47, pgs. 3897-3899, at pg. 3899, https://www.federalregister.gov/documents/2021/01/15/2021-01016/requirements-for-certain-transactions-involving-convertible-virtual-currency-or-digital-assets#p-22.

[20] For example, CVCs such as Monero and Zcash have functionalities that can shield this information from passive blockchain viewers. See: Andrea O'Sullivan, "What are mixers and 'privacy coins'?" *Coin Center*, July 7, 2020, https://www.coincenter.org/education/advanced-topics/what-are-mixers-and-privacy-coins/.

[21] *Ibid*.

[22] *Ibid*.

[23] Elizabeth Stark, "Lightning Network," *Coin Center*, September 15, 2016, https://www.coincenter.org/education/key-concepts/lightning-network/.

[24] Aaron van Wirdum, "Taproot is coming: what it is, and how it will benefit Bitcoin," *Bitcoin Magazine*, January 24, 2019, https://bitcoinmagazine.com/technical/taproot-coming-what-it-and-how-it-will-benefit-bitcoin.

Technology neutrality and practicality aside, this data is highly sensitive. Even if it is only collected when readily available, the mere act of centralizing those data points and matching them with real human names in a database is extremely invasive of persons' privacy and will put users of this technology at real risk of harm. Should this data be improperly shared amongst FinCEN's public partners in law enforcement[25] or amongst FinCEN's private partners at financial institutions[26] it can be used to target otherwise innocent individuals for harassment or extortion.[27] Should this data be leaked by FinCEN employees[28] it can be used to blackmail Americans. Should this data be lost in a hack[29] it can be used to enable further cyberattacks against Americans and large institutions dealing in CVC. There is no responsible way to aggregate and maintain this data. It should not be collected to begin with except in narrow circumstances warranting such invasive surveillance (*i.e.* when there is individual suspicion of a crime and a judge authorizes a warrant for its collection).

CVC technology is rapidly trending towards the creation of true electronic cash (digital money that leaves no trace of its movement through the world).[30] This trend is inevitable and it is a boon for human dignity and freedom.[31] Invasive surveillance techniques beyond simple CTR reports will only accelerate that progress, as more individuals will voluntarily choose to use more private CVCs and CVC transaction-types to smartly avoid being listed in a vulnerable government database through no wrong-doing or fault of their own. Electronic cash should be treated no different than physical cash and, therefore, VCTRs should be as similar as possible to existing CTRs.

---

[25] Jason Leopold and Jessica Garrison, "US Intelligence Unit Accused Of Illegally Spying On Americans' Financial Records," *Buzzfeed News,* October 6, 2017, https://www.buzzfeednews.com/article/jasonleopold/us-intelligence-unit-accused-of-illegally-spying-on.

[26] Benjamin Powers, "How FinCEN Became a Honeypot for Sensitive Personal Data," *CoinDesk*, December 10, 2020, https://www.coindesk.com/fincen-files-honeypot.

[27] Cyrus Farivar and Joe Mullin, "Stealing bitcoins with badges: How Silk Road's dirty cops got caught," *Ars Technica*, August 17, 2016, https://arstechnica.com/tech-policy/2016/08/stealing-bitcoins-with-badges-how-silk-roads-dirty-cops-got-caught/.

[28] "FinCEN Files," International Consortium of Investigative Journalists, https://www.icij.org/investigations/fincen-files/.

[29] Many U.S. federal agencies, including the Treasury Department, recently succumbed to a major hack of the SolarWinds software suite. *See*: David E. Sanger, Nicole Perlroth, and Eric Schmitt, "Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit," *New York Times*, December 14, 2020, https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html.

[30] Jerry Brito, "The Case for Electronic Cash," *Coin Center*, February 2019, https://www.coincenter.org/the-case-for-electronic-cash/.

[31] *Ibid*.

How to implement a technology-neutral and reasonably data-minimized VCTR

FinCEN can easily create a level playing field between legacy transactions and virtual currency transactions, do less harm to the privacy rights of Americans, and lower its own administrative burdens by simply adapting the existing CTR Form 104[32] to work in the context of both virtual currency and legacy transactions. This can be accomplished by mirroring current "foreign cash" reporting requirements with identical convertible virtual currency requirements and by providing simple definitions and instructions related to the filing of CTRs in the context of CVC transactions. Rather than create a *de novo* VCTR, Coin Center urges FinCEN to simply adopt the following minimal alterations to Form 104 and its accompanying instructions to Financial Institutions (all new language italicized):

A) Amend the 26a transaction type in Part II from "Foreign cash in _____" to to include both "Foreign cash *or CVC* in _____"; alter 27a from "Foreign cash out _____" to "Foreign cash *or CVC out* ____"; alter 29 "Foreign Country _____" to "Foreign Country or *CVC type* _____"

B) Add three new items in the general instructions to define CVC (following previous FinCEN definitions), explain which CVC transactions are subject to reporting, and mirror the current foriegn cash exchange rate instructions:

> ***Convertible Virtual Currency (CVC)***
> *The term "virtual currency" refers to a medium of exchange that can operate like currency but does not have all the attributes of "real" currency, as defined in 31 CFR § 1010.100(m), including legal tender status. Convertible Virtual Currency (CVC) is a type of virtual currency that either has an equivalent value as currency, or acts as a substitute for currency, and is therefore a type of "value that substitutes for currency."*
>
> ***Convertible Virtual Currency Transactions Subject to Reporting***
> *This Currency Transaction Report should be filed for any CVC transaction received by the reporting institution on behalf of one or more customers if the initiator of the transaction is not a Financial Institution or if the reporting institution cannot determine whether the initiator is a Financial Institution, and if the transaction involves more than $10,000 in CVC (See "CVC exchange rates"). This report should also be filed for any CVC transaction initiated by the reporting institution on behalf of one or more customers if the recipient of the transaction is not a Financial Institution and if the transaction involves more than $10,000 (See "CVC exchange rates"). This report should NOT be filed for CVC transactions initiated by a Financial Institution and received by a Financial Institution, however such transactions may be subject to*

[32] Available at: https://www.irs.gov/pub/irs-tege/fin104_ctr.pdf.

Suspicious Activity Report filings, Travel Rule requirements, and/or other applicable rules.

CVC exchange rates
If CVC is a part of a transaction that requires the completion of a CTR, use the exchange rate in effect for the business day of the transaction to compute the amount, in US dollars, to enter in item 26/27. The source of the exchange rate that is used will be determined by the reporting institution.

C) adjust the language in "Part I - Person(s) Involved in Transactions" to clarify that these transactions are to be treated within reports as cash deposits and withdrawals are treated, and to be clear that these reports do not require additional unwarranted surveillance:

PART I - Person(s) Involved in Transaction(s)
Section A must be completed. If an individual conducts a transaction on his own behalf, complete Section A and leave Section "B" BLANK. If an individual conducts a transaction on his own behalf and on behalf of another person(s), complete Section "A" for each person and leave Section "B" BLANK. If an individual conducts a transaction on behalf of another person(s), complete Section "B" for the individual conducting the transaction, and complete Section "A" for each person on whose behalf the transaction is conducted of whom the financial institution has knowledge. *As with cash transactions, an individual may conduct transactions using Convertible Virtual Currency on his own behalf, on his own behalf and on behalf of another person(s), or on behalf of another person(s). In each case, Sections "A" and "B" should be completed accordingly as if these transactions were cash withdrawals or deposits. The reporting institution is NOT obligated to independently investigate or surveil their customer, other third parties, or any non-public CVC network data, in order to obtain or verify this information.*

D) Adjust the instructions for Items 26, 27 to clarify the expansion of these fields to CVC:

Items 26 and 27. Total Cash In/Total Cash Out.
In the spaces provided, enter the total amount of currency *and/or CVC* received (Total Cash In) or total currency *and/or CVC* disbursed (Total Cash Out) by the financial institution. If foreign currency *or CVC* is exchanged, use the U.S. dollar equivalent on the day of the transaction (See "Foreign exchange rates" *and "CVC exchange rates"*), and complete item 26a or 27a, whichever is appropriate.

> If less than a full dollar amount is involved, increase that figure to the next highest dollar. For example, if the currency totals $20,000.05, show the total as $20,001.00.
>
> **Items 26a and 27a. Foreign cash *or CVC* in/Foreign cash *or CVC* out.** If foreign currency *or CVC* is exchanged, enter the amount of foreign currency *or CVC* (Do not convert to U.S. dollars) in items 26a and 27a. Report country of origin *or CVC type* in item 29.

E) Adjust the instructions for Item 29 to allow reporting institutions to report CVC type in a flexible but accurate manner (given the present absence of any authoritative global standard for particular CVC names and symbols):

> **Item 29. Foreign Country *or CVC Type*.** If items 26a and/or 27a are completed indicating that foreign currency *or CVC* is involved, check Item 29 and identify the country *or CVC type*. If multiple foreign currencies *or CVC types* are involved, check box 36 and identify the additional country(s), *CVC types*, and/or currency(s) involved. *CVC types should be recorded with as much precision as reasonably possible and may include commonly used names (e.g. Bitcon) as well as symbols (e.g. BTC). The choice of names and/or symbols used to describe CVC type will be determined by the reporting institution.*

Finally, we note that implementation of a VCTR through the existing Form 104 avoids the creation of unnecessarily complicated bespoke compliance obligations proposed in the recent notice of proposed rulemaking. For example, the existing Form 104 standards for aggregation are straightforward: a bank must file if transactions total more than $10,000 "during any one business day" while other financial institutions are directed to treat each calendar day as a "business day." [33] The proposed rule, on the other hand, would mandate a divergent aggregation rule wherein the "24-hour period begins from the first unreported transaction."[34] No explanation is offered for why CVC transactions warrant this divergent and seemingly arbitrary alternative standard. Any financial institution dealing in both CVC and legacy currencies would, under the proposed rule, be obligated to develop entirely separate compliance processes at some cost and without any perceivable benefit. Again, rather than complicate compliance efforts and create further privacy and data security risks, FinCEN, if it insists on further warrantless surveillance, should simply use the existing warrantless surveillance standards and instructions found in Form 104.

---

[33] *Ibid*.

[34] https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28437.pdf

FinCEN must perform a cost-benefit analysis between this data-minimized VCTR and more invasive approaches

We urge FinCEN to consider this data-minimized alternative to the proposed VCTR. As Congress has instructed with respect to CTRs in general,[35] FinCEN should do a thorough cost-benefit analysis as between the proposed privacy-invasive VCTR and a simple alteration to the existing CTR Form 104 as we have proposed. Any reasonable analysis will consider the following:

1. Collection and retention of data beyond a simple CTR (*i.e.* matching customer names with recipient bitcoin addresses) will create unaddressable data security risks. Even with the best cybersecurity practices, hacks[36] and leaks[37] will be inevitable and the damage they inflict on innocent Americans will be irreversible.

2. Development of an internal protocol for securing this extremely sensitive data will require, itself, significant cost. Rules will need to be established for whether and when this extra sensitive data can be shared with other government agencies and with the private sector (sharing that is encouraged by existing laws[38]). It would be safer and cheaper to simply avoid collecting the data and triggering sharing obligations at the start.

3. Avoiding the collection of this data does not permanently foreclose its availability to law enforcement. Should a traditional CTR reveal that a person of interest is moving large amounts of money off of financial institutions in the form of CVCs, then FinCEN or other law enforcement can subpoena financial institutions for additional data and/or use blockchain analysis to augment the otherwise limited information in the CTR. Avoiding the collection of extra data *ex ante* of suspicion does not impoverish law enforcement. It simply protects innocent individuals who are not even under investigation or suspected of committing a crime.

4. Much of the data sought will already be reported in SARs or remain on file with financial institutions and be available to subpoena.

---

[35] *Supra* note 10.
[36] *Supra* note 28.
[37] *Supra* note 27.
[38] According to FinCEN, "Section 314(b) of the USA PATRIOT Act provides financial institutions with the ability to share information with one another, under a safe harbor that offers protections from liability, in order to better identify and report activities that may involve money laundering or terrorist activities." See: "Section 314(b) Fact Sheet," Financial Crimes Enforcement Network, December 2020, https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf.

5. Any CVC-specific reporting fields will be rapidly outdated as particularized information such as payment address or transaction ID may not exist in all versions of CVC protocols and may rapidly change or be made obsolete as these technologies improve. Adopting specific requirements today will create a technical debt in the future and lead to further costly and disruptive rulemakings and compliance practices at regulated financial institutions.

We respectfully request that FinCEN carefully review these issues and perform a bona fide cost benefit analysis before moving forward with a VCTR. Should a VCTR be inevitable, it must only include information found in traditional reports: customer name and amount moved into or out of the control of the reporting institution. The best way to accomplish this is to amend the existing CTR Form 104 as suggested in this comment. Thank you for your extension of this rulemaking and your serious consideration of the privacy rights of Americans utilizing these important new technologies.

Sincerely,

Peter Van Valkenburgh

Director of Research
Coin Center