Re: FINCEN-2020-0020; RIN 1506-AB47

No Author Given

No Institute Given

Abstract. This short paper is the public comments provided by Payward, Inc. ("Payward") to the Financial Crime Enforcement Network's (FinCEN) proposed rulemaking on anti-money laundering requirements regarding convertible virtual currency, and is reformatted for the discussion at CoDecFin2021. Payward does business as 'Kraken'. Kraken believes the proposed rule would be bad for America and for the world. It would be a substantial departure from existing law. It would require enormous ongoing expenditure of resources by exchanges. It would cut off the poor from critical money flows. It fails to consider even the most basic costs or timing of implementation. It virtually guarantees that the evidence available to law enforcement today will be placed outside their reach tomorrow. Kraken's original comment letter is available at https://kraken.docsend.com/view/2fxvkmn77uz9bqjq. FinCEN's proposed rule notice is available at https://home.treasury.gov/news/press-releases/sm1216.

Keywords: Cryptocurrency, un-hosted wallet, regulation, anti-money laundering (AML)

Date: January 4, 2021

1 Introduction

Payward, Inc. ("Payward") is pleased to submit these comments on the Department of Treasury's Financial Crime Enforcement Network ("FinCEN") proposed rule notice ("NPRM") [1] to increase the anti-money laundering ("AML") requirements for money service businesses ("MSBs") and banks that provide services to users of convertible virtual currency ("CVC") and legal tender digital assets ("LTDA") and to modify the definition of "monetary instruments" in the Bank Secrecy Act ("BSA") to include CVC and LTDA for the purposes of AML reporting, recordkeeping, verification and other requirements.

Payward does business as 'Kraken'. Kraken's primary business is the operation of an online cryptocurrency exchange. Kraken's operations in the United States are carried out through Payward Ventures, Inc., a FinCEN-registered MSB. In addition, an independently- operated Kraken affiliate, Payward Financial, Inc., recently obtained the country's first special purpose depository bank charter from the State of Wyoming.

[1] 85 Fed. Reg. 83840 (December 18, 2020)

Kraken believes the NPRM proposes a substantial departure from existing law. It requires enormous ongoing expenditure of resources by regulated entities. It cuts off the poor from critical money flows. It fails to consider even the most basic costs or timing of implementation, and capriciously subjugates the rights of MSBs that offer hosted wallet services to those of traditional MSBs that do not. It virtually guarantees that the evidence available to law enforcement today will be placed outside their reach tomorrow.

Seemingly recognizing these deficiencies, FinCEN timed the NPRM's publication to avoid scrutiny and all but eliminate public input. The NPRM was published on Friday, December 18, 2020, with a return date for comments just fifteen days later, on Monday, January 4, 2020, with the holidays and New Year occurring during this limited window. Fifteen days of consideration is enough time to know that the costs of implementing the proposed rule would be staggering. It is enough time to know that the ongoing loss of access to information by US law enforcement would be substantial. It is enough time to know that eliminating services to America's most vulnerable individuals would be devastating. It is even enough time to know that the costs of these consequences could be calculated and understood, but fifteen days is not enough time to actually calculate them and understand them.

All we understand is that the proposed rule will chill innovation, cut off life-saving payment flows to homeless, unhoused, migrant and refugee populations, create risks to cryptocurrency users, erode law enforcement's access to evidence, drive profitable businesses offshore - and provide almost no helpful information to FinCEN. It is quite clearly a politically- motivated piece of midnight rulemaking, the publication of which diminishes the trust we have placed in FinCEN, otherwise one of our country's most respected regulators. This proposed rule will utterly fail to achieve the stated aim of the NPRM, "to address the illicit finance threat created by one segment of the CVC market and the anticipated growth in LTDAs." [2]

This comment letter addresses the issues which Kraken is particularly well-placed to explain, given the limited time permitted.

2 The proposed reporting requirements generate limited new information for FinCEN while ignoring basic technology limits and creating a massive compliance burden.

2.1 Proposed Reporting Requirements in 31 CFR Â§1010.316

FinCEN proposes to "require banks and MSBs to file a report with FinCEN containing certain information related to a customer's CVC or LTDA transaction and counterparty (including name and physical address)." [3] The report would

[2] 85 Fed. Reg. 83840, at 83841.
[3] 85 Fed. Reg. 83840, at 83843.

be required when "a counterparty to the transaction is using an unhosted or otherwise covered wallet and the transaction is greater than $10,000" or whenever the transaction is one of multiple transactions in a 24-hour period between a hosted wallet and an unhosted wallet "that aggregate to value in or value out of greater than $10,000." [4]

Developing a process to support currency transaction reporting ("CTR") for all transactions (or group of transactions, per the structuring requirements) of $10,000 or more will present technological, operational and compliance challenges for Kraken that will take at least eighteen months for Kraken to develop and test and put into place with any confidence. Given more time than the fifteen days allotted for consideration, Kraken could improve this estimate, and project its financial impact as well.

To understand some of the technological challenges that make reporting (and therefore, recordkeeping) on cryptocurrency transactions difficult, FinCEN must understand that MSBs and banks serving CVC and LTDA customers must work within the confines of cryptocurrency technology, which does not inherently provide information regarding the counterparties to a cryptocurrency transaction. Indeed, the primary reason that law enforcement today has information regarding the individuals involved in cryptocurrency transactions is because MSBs and banks offer hosted wallet services, which FinCEN has defined as arrangements wherein "a financial institution may execute transactions on a blockchain on behalf of a customer using a private key controlled by the financial institution".[5]

While FinCEN has proposed exempting the reporting of transactions between two parties that both have hosted wallets, this exemption is of limited value because MSBs and banks often cannot even tell before the transaction is completed whether the beneficiary of the cryptocurrency transaction is interacting with cryptocurrency through an MSB or bank, or independently. The very nature of cryptocurrency technologies is that there is no central registry with which to identify the counterparty and the nature of that party's wallet, hosted or not. As such, without providing MSBs and banks that offer hosted wallet services with the time to understand exactly how much effort is involved in identifying whether the counterparty to the transaction is operating through a hosted wallet or not, the practical effect of pushing the rule forward as written is that MSBs and banks acting conservatively would need to report all transactions (or aggregated transactions) until such time as they were able to more readily discern whether a given counterparty operates through a hosted wallet.

To understand why this is true for a cryptocurrency exchange, consider Kraken's best guess at how compliance would work in practice. Prior to each outgoing transaction:

---

[4] Ibid.

[5] 85 Fed. Reg. 83840, at 83842.

- Every outgoing address would require pre-screening to determine if it is hosted or non- hosted. This relies on third-party blockchain analytics providers. In this very Notice, FinCEN states such analytics are "not a panacea."
  - This requires advanced integrations with 3rd party service providers in a real- time manner - a major undertaking for Kraken's product and engineering teams.
  - This requires corresponding connections to core transaction processing systems and user interface touchpoints to ensure the correct workflow processes - another major undertaking for Kraken's product and engineering teams.
- If the address is hosted, Kraken must identify if the "host" is located in a jurisdiction that is acceptable to FinCEN per its Foreign Jurisdiction List. This list has yet to be published and is open to frequent change.
  - This requires integration to download the updated list from FinCEN and integrate into a yet-to-be-built monitoring system developed specifically for this purpose. This is yet another major undertaking for Kraken's product and engineering teams.
- If hosted in an acceptable jurisdiction, Kraken must determine whether the host is properly registered or licensed according to local law:
  - This would require staffing additional legally-trained personnel to determine the legal requirements in each jurisdiction, and verify each entity's current status, a major undertaking for Kraken's legal and compliance teams.
  - Some form of whitelisting would then need to be developed and integrated into the payment gateways that MSBs utilize to ensure automation/efficient processing. This is yet another major undertaking for Kraken's product and engineering teams.
- If the wallet address is unhosted, Kraken would need to collect intended beneficiary name and address. It would need to screen this information for sanctions, PEP and negative news, and then "enhanced controls" would need to be implemented.
  - These steps would require a new user interface and would create attendant customer friction.
  - It would also require systemic integration with 3rd party vendor list screening services and automated transaction interdiction based on the results. This is yet another major undertaking for Kraken's product and engineering teams.
  - Additional staffing would be needed 24/7/365 to ensure the high rates of false positives that are inherent to these 3rd party vendor solutions could be cleared in a timely manner or else risk diminishing the value

of the underlying blockchain technology altogether. This is yet another major undertaking for Kraken's compliance team.

- All transactions would need to be assigned a transaction code that identified them as either reportable or non-reportable for purposes of compliance with the proposed rule, then a new reporting system would need to be developed to identify aggregated transactions on a rolling 24 hour period. This is yet another major undertaking for Kraken's product and engineering teams.

    - Special methodology would have to be developed to figure out reporting requirements when numerous transactions over a longer than 24 hour period occurred. This type of scenario is not normally at issue in traditional banking because cryptocurrency operates 24/7/365. This is yet another major undertaking for Kraken's product, compliance and engineering teams.

- Due to the volume of potential reportable filings under the proposed rule, Kraken would need to plan and build an integration with a third party vendor solution, or develop a proprietary system, to connect to FinCEN for automated reporting. Alternatively, if the final rule permitted, Kraken could create reports that are able to be filed in batch format to avoid some staffing overhead.

    - A new team of analysts (and management staff) would be required to meet the reporting obligations and ensure that all timelines are met. This is yet another major undertaking for Kraken's product and compliance teams.

- New transaction monitoring rules would need to be developed to trigger sets of transactions that might be indicative of potential structuring.

    - Each alert would need to be reviewed and processed by qualified individuals in the AML investigative unit. Considering the high rates of false positives endemic to traditional banking institutions with structuring alerts, this burden would be considerable but would provide minimal benefit to AML investigations. This is yet another major undertaking for Kraken's compliance team.

- Kraken would need to hire additional systems analysts to ensure proper validation and alignment with management systems and controls. This is yet another major undertaking for Kraken's compliance team.

FinCEN requests input [6] on whether extending the 31 CFR Â§1010.316 requirement to transactions between hosted wallets would increase the compliance burden on MSBs. Practically speaking, compliance with the rule means that for every qualifying transaction, the MSB or bank must take time after the transaction has occurred to research and make a determination as to whether the

[6] 85 Fed. Reg. 83840, at 83851, Question 6.

recipient had a hosted wallet or not, and only then report the transaction. Accordingly, Kraken does not believe that reporting all transactions that meet the $10,000 or more threshold will increase compliance costs beyond the burdens already described above. Kraken does believe, however, that this profusion of reporting will not be useful to law enforcement.

In its questions regarding implications of the recordkeeping provisions, FinCEN has also asked for feedback on whether aggregating fiat and cryptocurrency transactions for these reporting requirement purposes would be beneficial. [7] In fact, combining fiat and cryptocurrency transactions would exponentially increase the burdens described above and would also increase the likelihood that any combination of $10,000 or more, regardless of what is occurring, will be reported to FinCEN. Without more time to study this question, Kraken can only opine that such reporting would dramatically increase the number of unhelpful reports made and therefore the information will not be useful to law enforcement due to the volume FinCEN will receive.

Finally, when fiat currency transactions are involved, the transactions of many corporations and other non-governmental entities are exempted from the $10,000 reporting threshold. [8] This standard primarily recognizes that such entities often have such high-dollar transactions and reporting them to FinCEN is not particularly useful for law enforcement. However, the NPRM proposes not extending the exemptions for transaction reporting to entities that would normally be exempt for fiat currency purposes. Based upon Kraken's experience with transactions made by corporations and other non-governmental entities, the same policy reasons for providing the exemption for fiat currency transactions apply to cryptocurrency transactions.

2.2 Recordkeeping, Verification and Other Requirements

The next major provisions of the proposed rule are related to recordkeeping and verification, requiring "banks and MSBs to keep records and verify the identity of their hosted wallet customers, when those customers engage in transactions with unhosted or otherwise covered wallets with a value of more than $3,000." [9]

The proposed rule references MSBs and banks maintaining "other counterparty information the Secretary may prescribe as mandatory on the reporting form for transactions subject to" the reporting requirements. [10] Yet, the reporting form was not included in the NPRM for industry participants to evaluate. Because FinCEN has demonstrated in the proposed rule that it does not seem to fully understand that MSBs and banks do not have the ability to modify or adapt cryptocurrency technology and that the information available on counterparties is limited, Kraken implores FinCEN and the Secretary of the Treasury to submit

[7] 85 Fed. Reg. 83840, at 83851, Question 9.
[8] 31 CFR 1020.315.
[9] 85 Fed. Reg. 83840, at 83848.
[10] 85 Fed. Reg. 83840, at 83861, referencing proposed section 1010.410(1)(vii).

any additional "counterparty information" requirements for public review and comment.

In addition, the proposed rule references MSBs and banks maintaining, as part of the recordkeeping requirements, "[a]ny other information that uniquely identifies the transaction, the accounts, and to the extent reasonably available, the parties involved." [11] In the cryptocurrency context, this unworkably broad provision to maintain any uniquely identifying information could require MSBs and banks to maintain entire cryptocurrency ledgers - which minutely detail unique identifying information about each and every transaction. Maintaining that much information for each and every transaction is untenable. FinCEN should reconsider what information it actually requires in this provision and ask only for that information. Furthermore, collecting the data and maintaining the data are distinct requirements. If the data is available to the MSB or bank, then the information could be collected, but building the systems to maintain such data while maintaining privacy and security compliance will take time and effort. FinCEN has already conceded that costs of compliance with the rule for MSBs in particular, most of which are small businesses, will be significant. Expansion of data to be tracked, retained and made available to law enforcement will just add to the overwhelming burden of the rule.

In the questions posed, FinCEN also requests information regarding requiring MSBs or banks to not only collect available counterparty information from its customer, but to actually verify counterparty information before allowing a transaction to go forward. [12] As described above, MSBs or banks are limited due to the very nature of cryptocurrency technologies in their ability to even obtain counterparty information, much less verify that information. As such, a requirement that 100% of all hosted wallet transactions must have counterparty information verified by the MSB or bank before the transaction can move forward, without any ability for the MSB or bank to otherwise risk-weight the transaction, would effectively cause the majority of affected cryptocurrency transactions to stop altogether.

3 The definition of "monetary instruments" fails to consider real-world uses of digital assets.

FinCEN asks whether its proposed definition of "monetary instruments" ought to include "convertible virtual currency". [13] FinCEN's proposed definition of "convertible virtual currency" is so broad that it includes securities, commodities and other tokenized investment products. Thus, the better question is whether the proposed definition of "convertible virtual currency" (and therefore "monetary instruments") ought to capture investments. The answer is No, but the NPRM fails to consider this foundational, jurisdictional question.

[11] Ibid, referencing proposed section 1010.410(1)(viii).
[12] 85 Fed. Reg. 83840, at 83851, Question 15.
[13] 85 Fed. Reg. 83840, at 83851, Question 1.

FinCEN first introduced the concept of a "convertible virtual currency" in its March 2013 guidance. [14] At the time, actual users of what FinCEN called CVC, and actual providers of CVC services - those with actual knowledge of the asset class - were baffled by its breadth: The definition included Bitcoin, to be sure, but it also purported to include any asset that could be represented on an open, permissionless decentralized electronic ledger.

Few such assets existed in 2013, so the guidance was less of a problem. Today, thousands and potentially tens of thousands of these assets exist. The CVC definition has not aged well, particularly because these assets are not all currencies. Indeed, the Securities and Exchange Commission has argued - and federal courts have confirmed - that some are actually securities. [15] The Commodity Futures Trading Commission has found - and federal courts have confirmed - that some are commodities. [16]

By conflating "monetary instruments" with "convertible virtual currency", FinCEN now claims jurisdiction over a much broader range of assets than ever before. [17] This represents a new challenge to compliance personnel: What does structuring mean in the case of tokenized securities? Tokenized commodity derivatives? What activity ought to be suspicious? Worse, it represents an unprecedented expansion of FinCEN's regulatory perimeter. FinCEN offers no justification for claiming jurisdiction over securities and commodities. It seeks simply to do so in a midnight rulemaking, with fifteen days (minus Christmas and New Year's Day) for the public to comment.

4 The proposed rule imposes greater compliance burdens on MSBs that provide hosted wallet services than other MSBs.

Kraken believes it is important to raise the issue of parity - parity between how fiat currencies and cryptocurrencies are managed, and parity among MSBs. Traditional financial services regulation takes as a guiding tenet that a regulatory scheme should apply the same rules for all involved financial institutions, unless compelling reasons dictate imposing additional obligations on certain kinds of financial institutions. This concept of parity is intended to ensure fair competition among financial institutions and to encourage a variety of financial institutions

[14] FinCEN Guidance, FIN-2013-G001. Available at: https://www.fincen.gov/sites/default/files/shared/FIN- 2013-G001.pdf

[15] See, e.g., In re Tomahawk Exploration LLC, Securities Act Rel. 10530 (Aug. 14, 2018)

[16] See, e.g., CFTC v. McDonell,18-CV-361 (E.D.N.Y. Mar. 6, 2018) and In the Matter of BFXNA Inc d/b/a BITFINEX. CFTC Docket No. 16-19, June 2, 2016.

[17] For example, see FinCEN's guidance in 2019 regarding the CVC term and its applicability: FIN-2019- G001. Available at: https://www.fincen.gov/sites/default/files/2019- 05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf

to support various aspects of the economy and to otherwise achieve important economic and societal goals.

The proposed rule in the NPRM shatters parity among MSBs, in terms of the weight of obligations sought to be hung about the yoke of MSBs that offer hosted wallet services. Transactions conducted by MSBs not involved in cryptocurrency generally have a similar risk profile to that of cryptocurrency transactions, without the added benefits of traceability and transparency that cryptocurrency ledgers provide to law enforcement. And similarly, often the transactions conducted by MSBs not involved in cryptocurrency do not require (and the MSBs are not required to maintain) clear information about the beneficiaries of the transactions. Yet, MSBs that offer hosted wallet services and that already provide more information than ever to law enforcement (especially compared to fiat transactions managed by MSBs not involved in cryptocurrency) are being required to comply with ever more burdensome AML provisions. FinCEN has not provided any information or justification regarding why the concept of parity among MSBs should be abandoned, particularly when cryptocurrencies offer indelible public ledgers of all transactions. Instead, the NPRM takes the bizarre position that the proposed rule is consistent with existing requirements. Kraken believes that destroying parity among MSBs in this manner will only chill the development of cryptocurrency technologies in the United States.

5 The proposed rule fails to consider effects on homeless, unhoused, migrant, and refugee populations.

FinCEN's rules already prohibit financial institutions from opening accounts for homeless, unhoused and refugee populations who do not have physical mailing addresses. [18] The proposed rule would now prohibit those who are fortunate enough to have accounts from even sending money to these people, if that money is a CVC.

Twenty-five percent of US households are unbanked or underbanked. [19] Still more homeless and unhoused cannot even qualify as "households", and would add to this proportion. Refugees and migrant populations, whether within or outside the US but still dependent upon our financial system add to this number even further. Existing requirements prohibit financial institutions from opening accounts for these people. Existing requirements do, however, permit them to receive money from those who can afford to pay account maintenance fees and live in neighborhoods that attract physical branches. The proposed rule would go beyond existing requirements to literally outlaw people sending money to the less fortunate using their financial institutions.

[18] 31 CFR Â§103.121, et seq., and 81 Fed. Reg. 29398 (May 11, 2016).

[19] See, e.g., https://www.cnbc.com/2019/03/08/25percent-of-us-households-are-either-unbanked-or-underbanked.html

The NPRM does not rebut or distinguish these claims. It simply fails to consider them. The public could, in fact, quantify and project the rule's impact on these vulnerable populations. FinCEN simply elected not to provide sufficient time to do so. This oversight is glaring.

6 The proposed rule will create a more functional, more convenient shadow cryptocurrency system that is completely opaque to US Anti-money laundering efforts.

A unique feature of cryptocurrency networks makes the consequences of this proposed rule particularly worrisome: These networks are permissionless. Unlike existing financial systems, people do not need to use financial institutions to use their money. Customers who want to send a wire transfer use a bank because they must. Customers who want to send a bitcoin use an exchange because it is convenient. These customers could instead choose to maintain the private key for cryptocurrencies they own and transact without the aid of an MSB, simply by interacting directly with the cryptocurrency network of their choice.

Customers instead use Kraken and other MSBs because maintaining a cryptocurrency private key can be difficult. Compared to financial institutions, individuals usually lack the necessary security to protect the digital file containing the private key. This leaves customers open to security breaches, and in some real-life anecdotes, to private keys and the associated funds lost forever from misplaced notebooks or crashed hard drives. MSBs and banks provide a convenient and secure alternative for CVC and LTDA customers. But, when regulatory requirements make this convenient and secure alternative burdensome, inefficient, and invasive, then even responsible United States citizens transacting with CVC and LTDA will eventually avoid the MSBs and banks and take matters into their own hands. This cannot happen in traditional financial services. After all, you can't send a wire transfer without a financial institution.

The proposed rule is only effective when customers are interested in using hosted wallet services. The proposed rule makes the offering of hosted wallet services burdensome, invasive, and expensive. Customers are not interested in using burdensome, invasive, or expensive services. Over time, the proposed rule will influence customers to cease using MSBs and fewer cryptocurrency service providers will provide services in the United States. Because of cryptocurrency networks' permissionless nature, though, this will not stop criminals from using cryptocurrency in the United States. United States law enforcement and intelligence agencies will have less information regarding either the sender or the recipient of cryptocurrency transactions. The proposed rule will render this country's robust and effective AML regulatory regime increasingly fragile and ineffective.

Indeed, every limitation on individuals' ability to transact using cryptocurrency MSBs fuels a phenomenon that cannot exist in traditional money services: It

splits cryptocurrency users into two incompatible halves, one half completely opaque to law enforcement. In one half, all transactions would be between verified parties who use MSBs. In the other half, all transactions would be between unverified parties who could not send transactions to or from MSBs. This latter half of the ecosystem would have no obligation to file suspicious activity reports, adopt AML policies, or conduct anti-money laundering checks at all. They would have no obligation to respond to law enforcement except via subpoena, if they could ever be found. The proposed rule's burdensome requirements would accelerate the creation of an entire economy opaque to law enforcement, and growing larger with every new limitation on MSBs.

7 FinCEN should revise the proposed rule and provide iterative supplemental comment periods.

The NPRM fails to consider basic definitional premises of what is a CVC, even when the issue is today being hotly debated in the courts. It fails to consider the costs of implementation and compliance. It fails to consider the consequences to vulnerable populations. It fails to consider the loss of access to information to be suffered by law enforcement. Then, even though these impacts are, by and large, quantifiable and understandable, it fails to provide sufficient time for the public to quantify and understand them.