Re: FinCEN Docket Number FINCEN-2020-0020; RIN 1506-AB47; Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets

Ryan Taylor, CEO

Dash Core Group

Abstract. Dash is **NOT** an anonymity-enhanced cryptocurrency.

Keywords: Blockchain, KYC, AML, Compliance, Information Security, Regulation Awareness, Anonymity-Enhanced Cryptocurrency, AEC, FinCEN

Date: January 4, 2021

1 Introduction

Dash Core Group ("DCG") appreciates the opportunity to submit this letter for consideration by the Financial Crimes Enforcement Network ("FinCEN") with respect to the Notice of Proposed Rulemaking ("NPR"), published on December 23, 2020, titled "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets." See 85 FR 83840.

We offer this letter for a very specific purpose. The NPR describes at length the government's concerns that certain segments of the convertible virtual currency ("CVC") market create an illicit finance threat. In particular, the NPR's background section identifies anonymity-enhanced cryptocurrencies ("AECs") as a money laundering risk, and specifically names the Dash cryptocurrency as an AEC "that inhibit[s] investigators' ability both to identify transaction activity involving blockchain data and to attribute this activity to illicit activity conducted by natural persons." 85 FR 83844.

This characterization of the Dash cryptocurrency is wrong. It misunderstands how the Dash cryptocurrency works. It ignores public statements by neutral third party experts- including the prominent blockchain analysis company Chainalysis, which the U.S. government itself often uses in its investigations-that transactions involving the Dash cryptocurrency can be both identified and attributed. And this characterization is having a material, negative impact on the Dash network's operations, as cryptocurrency exchanges around the world have begun delisting the Dash cryptocurrency based on the U.S. gov-

ernment's repeated (and mistaken) assertions that Dash is a money laundering risk.

DCG strongly opposes the use of cryptocurrencies for illicit purposes. Indeed, we have worked productively with law enforcement agents when they have approached us to advance their legitimate investigations. Moreover, we met with officials at FinCEN in June 2020 to describe how the Dash network works, and why any characterization of the Dash cryptocurrency as a money laundering risk is flawed. Nonetheless, the mis-characterization of Dash in official U.S. government documents continues. This arbitrary and capricious state of affairs is unacceptable, and it is significantly impacting the Dash network's operations. **We respectfully ask you to strike any reference to Dash in any future iterations of (or documents relating to) this Rule.**

2 Dash Is Not An Anonymity-Enhanced Cryptocurrency

Dash is a leading cryptocurrency network focused on payments. [1] A fork of Bitcoin's code, the Dash network is a user-operated network whose most typical use case is as digital cash for everyday transactions. Payments are near-instant, easy, and secure; users can purchase goods at thousands of merchants, and can trade Dash at major exchanges and brokers around the world.

We should emphasize the most important point upfront: ***Dash's network, just like Bitcoin's, features a transparent, auditable blockchain that does not have any hidden addresses or hidden transaction details. All transactions list the complete set of inputs, outputs, addresses, and amounts.***

We are, accordingly, at a loss for why official U.S. government documents continue to mislabel Dash as an AEC that is routinely used as a vehicle for money laundering and other illicit activity. [2] Most likely, those who view Dash as a money laundering risk are basing their assumptions on old (and flawed) information. It is true that Dash's founder-who is no longer associated with the project,

[1] DCG is distinct from the Dash network, and is one of the many entities serving that network. DCG is the largest software development organization for the Dash network and is primarily tasked with development of the protocol. We also engage in business development and marketing efforts that benefit the network. Other software development teams independent of DCG also perform work for the network.

[2] In addition to FinCEN's NPR, the U.S. Department of Justice recently issued an influential report that publicly (and erroneously) named Dash as an AEC that employs "non-public or private blockchains that make it more difficult to trace or to attribute transactions," "may undermine the AML/CFT controls used to detect suspicious activity by MSBs and other financial institutions, and may limit or even negate a business's ability to conduct AML/CFT checks on customer activity and to satisfy B[ank] S[ecrecy] A[ct] requirements." U.S. Department of Justice, Cryptocurrency Enforcement Framework (Oct. 2020) at 4, 41, available at: `https://www.justice.gov/ag/page/file/1326061/download`.

and has not been for almost four years-announced, shortly after Dash's launch in 2014, an initial focus on enhancing the pseudonymity of Bitcoin through an implementation of CoinJoin, and rebranded the coin (which then was called Xcoin) as "Darkcoin." This early decision branded Dash in a negative light and encouraged sensational press coverage depicting Dash as a cryptocurrency that facilitated illegal activities. Since mid-2014, however, the project focus has pivoted significantly. The coin was renamed "Dash" in March 2015 to reflect the network's new focus on providing its users with payment speed and efficiency (rather than privacy/anonymity), as embodied in its popular "InstantSend" feature. Speed, efficiency, and a superior user experience remain Dash's focus, but unfortunately the coin's legacy privacy/anonymity reputation lingers, particularly in the media. [3]

As we explained to representatives of FinCEN in June 2020, Dash is not an AEC because its privacy feature is simply a branded implementation of non-custodial CoinJoin, a privacy- enhancing technique that adds complexity to transactions that can be performed on any transparent blockchain. That is, unlike many other privacy solutions, CoinJoin transactions do not require any modifications to the Bitcoin protocol upon which Dash is based.

Notably, third-party experts agree with our assessment. For example, Chainalysis, a reputable company that both FinCEN and the Department of Justice use to combat money laundering, terrorist financing, and other illicit cryptocurrency uses, issued a statement (without any prompting from us) when, in mid-2020, it launched coverage of Dash. As Chainalysis declared:

"We just launched support for two notable cryptocurrencies in Chainalysis Reactor and KYT (Know Your Transaction): Dash and Zcash. As two of the most popular so-called "privacy coins"-cryptocurrencies with privacy enhancing features encoded into their protocols-they account for over 1.5 billion of reported daily trading volume.

You may be wondering how Chainalysis products could support privacy coins. Isn't the whole purpose of privacy coins to make transactions impossible to trace?

[3] For example, the popular Investopedia website lists Dash as the "#3" "privacy-oriented cryptocurrency," whose "PrivateSend feature" supposedly "obscur[es] the origin of your funds"-though the website does acknowledge that certain settings allow for users "to remain within their countries' regulatory standards." Investopedia, "Six Private Cryptocurrencies," available at: https://www.investopedia.com/tech/five-most-private-cryptocurrencies/ (last updated Dec. 24, 2020). For the reasons expressed in this letter, Investopedia's characterization is mistaken. We address the "PrivateSend" feature later in the text of this letter.

That's an oversimplification, in that it misunderstands both the privacy features coins like Dash and Zcash offer and how users actually utilize those features in everyday transactions." [4]

The statement goes on to explain that Dash's "most notable privacy modification [from Bitcoin] is its PrivateSend functionality." PrivateSend is "a branded implementation of the CoinJoin protocol . . . as a way to obscure the origin of funds." (As Chainalysis notes, however, "PrivateSend is optional," and "Dash transactions are unmixed by default.") The statement then describes how PrivateSend works from a technical perspective; the key takeaway point is this: "It's possible to perform mixing transactions that are functionally identical to PrivateSend on other technologically similar cryptocurrencies. This means from a technical standpoint, Dash's privacy functionality is no greater than Bitcoin's, making the label of 'privacy coin' a misnomer for Dash. In fact, independent wallet softwares provide more advanced forms of CoinJoin that are being used with major cryptocurrencies not labeled as privacy coins, such as Bitcoin, Bitcoin Cash, and Litecoin." [5] In other words, according to Chainalysis-the same company that the U.S. Department of Justice has publicly lauded on multiple occasions as a trusted private sector partner in the fight against illicit uses of cryptocurrency [6] -Dash's privacy features make it no harder, and in certain circumstances easier, to trace than Bitcoin. And, of course, no knowledgeable person would suggest that the use of Bitcoin raises insuperable challenges to law enforcement to confront and address the public safety and national security risks outlined in the NPR.

In an effort to demonstrate the similarities between the "digital trails" left by transactions conducted using Dash and those using Bitcoin, DCG in May 2019 took the initiative to conduct "PrivateSend" transactions on the Bitcoin network,

[4] Chainalysis, "Introducing Investigation and Compliance Support for Dash and Zcash," June 8, 2020, available at: https://blog.chainalysis.com/reports/introducing-chainalysis-investigation-compliance-support-dash-zcash.

[5] Id. (emphasis added).

[6] See, e.g., U.S. Dep't of Justice, Press Release, "United States Files A Civil Action To Forfeit Cryptocurrency Valued At Over One Billion U.S. Dollars," Nov. 5, 2020, available at: https://www.justice.gov/usao-ndca/pr/united- states-files-civil-action-forfeit-cryptocurrency-valued-over-one-billion-us (thanking Chainalysis by name); U.S. Dep't of Justice, Press Release, "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns," Aug. 13, 2020, available at: https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns (same); U.S. Dep't of Justice, Press Release, "Three Individuals Charged For Alleged Roles In Twitter Hack," July 31, 2020, available at: https://www.justice.gov/usao-ndca/pr/three-individuals-charged-alleged-roles-twitter-hack

and compared them to transactions using Dash. Here are links to the Bitcoin "PrivateSend" transactions.[7]

And here are links to the Dash "PrivateSend" transactions [8]

Each transaction block includes 20 publicly-displayed input and output addresses, and reflects identical transaction amounts. The blocks are identical in the information they reveal and there is absolutely no distinction between them!

In sum, Dash is a transparent, analyzable blockchain indistinguishable from Bitcoin in its functionality. Dash's PrivateSend feature is simply a branded implementation of non- custodial CoinJoin available on most public blockchains. All transaction inputs, outputs, addresses, and amounts are fully visible on the Dash blockchain for all transactions.

Of course, none of this is news to FinCEN; we covered these points in detail during our June 2020 meeting with nearly a dozen representatives across the agency's various divisions. Unfortunately, we have heard nothing from FinCEN since then. Instead, despite clear evidence to the contrary, the agency appears to have adopted the plainly erroneous view that Dash represents a money laundering risk.

3 Dash Is Rarely, If Ever, Used For Illicit Activities Or In Connection With Darknet Marketplaces

Not only is Dash a transparent, analyzable blockchain indistinguishable from Bitcoin in its functionality; it actually poses a lower risk than Bitcoin when it comes to illicit usage. First, there is no evidence that Dash is used for illicit purposes. In a recent Rand Corporation analysis of DarkWeb cryptocurrency usage, for example, Dash accounted for only 0.05% of identified cryptocurrency wallets [9]

[7] See Bitcoin Transaction through PrivateSend: `https://btc.cryptoid.info/btc/tx.dws?2e9aa4e7c7aa704055adc7ce396533164a097515189a30f1e9c8fa73b21dc174.html`

[8] See links to Dash PrivateSend transactions for comparison to Bitcoin "PrivateSend" transactions here at: `https://chainz.cryptoid.info/dash/tx.dws?a8656b7655c14445c652d8e5e27a6155e8a39aa792f99210607437737999a945.html`

[9] See Erik Silfversten, et al., Exploring the use of Zcash cryptocurrency for illicit or criminal purposes," Rand Corp., 2020, at 23 (Figure 3.7), available at: https://www.rand.org/pubs/research_reports/RR4418.html. As this report observes, "[S]ome commentators believe that due to their privacy enhancing features, altcoins such as Zcash (as well as Monero, Dash and Litecoin) represent notable competitors for Bitcoin with illicit users on the dark web." Id. at 12. The report concludes, however, that "little empirical evidence or research exists in support of this claim." Id. While we would disagree with the ill-informed commentators referenced in the report, who believe, without evidence, that Dash is an "altcoin" whose users tend towards criminality, we concur fully with the reportâs assessment that the use of Dash on illicit darknet marketplaces is negligible.

Second, Dash does not support advanced forms of CoinJoin such as Chaumian CoinJoin, which is present on the Bitcoin network. Finally, Dash does not support off- chain transactions that are not auditable on-chain. To reiterate the point once again: All transaction inputs, outputs, addresses, and amounts are fully visible on the Dash blockchain for all transactions.

4 The U.S. Government's Mischaracterization of Dash Has Had a Significant, Material, and Adverse Impact.

The public naming and shaming of Dash as an AEC (or "privacy coin") in FinCEN's NPR (as well as earlier in the fall of 2020 in the Department of Justice's "Cryptocurrency Enforcement Framework") has had a hugely negative impact on the project. This impact is real, and it has affected multiple aspects of our users, DCG's business, and the individuals involved in the project.

First, regulators around the world look to the United States as a regulatory leader in the innovative space of cryptocurrencies. As the U.S. government continues to perpetuate a false narrative that Dash is a privacy coin that poses an unacceptable money laundering risk, other countries are following its lead without independently corroborating its conclusions or conducting primary research into the issue. Specifically, Canada's FINTRAC, in December 2020, leveraged the U.S. Department of Justice report to define Dash as a privacy coin, stating that the use of Dash indicates a heightened risk of money laundering or terrorist financing-language that is eerily similar to DOJ's. [10]

In addition, we have in recent weeks received inquiries from regulators from other countries to whom DCG has taken the time to explain our optional privacy feature. The regulators are asking DCG to comment on the categorization of Dash as an AEC, when we specifically presented materials to them demonstrating why Dash is not an AEC. With their off-the-cuff (mis)characterizations of Dash, both FinCEN and the DOJ have undermined detailed, time- consuming facts and arguments DCG has conveyed to regulators outside of the United States, thereby sowing confusion.

Second, the categorization has had a significant negative business impact on Dash. We have learned that cryptocurrency exchanges that currently list or are considering listing Dash are now reviewing their policies to ensure that they are in compliance with the U.S. government's regulatory guidance. Apparently, relying on DOJ's and FinCEN's recent pronouncements, a number of exchanges have taken the additional step of delisting Dash in order to "derisk" themselves. For example, on January 1, 2021, Bittrex, one of the world's leading cryptocurrency exchanges, announced that it would delist Dash as of January 15, 2021.

[10] Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), "Money laundering and terrorist financing indicators â Virtual currency transactions," Dec. 2020, available at: `https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/indicators-indicateurs/vc_mltf-eng`

[11] No official explanation was given, but public reporting suggests that Bittrex's action is part of a broader trend wherein "exchanges around the world have been moving to delist coins that seek to preserve the privacy of their users as a way to be compliant with know-your-customer (KYC) and anti-money laundering (AML) regulations that are spreading around the world." [12]

Completely overlooked in all of this is the fact that Dash is not a "privacy coin," and that its use is perfectly compatible with KYC and AML regulations. Meanwhile, it is Dash's users and the members of its network who are left holding the bag for the U.S. government's mistake: for example, Dash's price immediately dropped by approximately 15% on news of its Bittrex delisting.

Finally, individuals associated with the Dash project have incurred significant reputational risk and harm as a result of the U.S. government's continued (mis)characterization of the Dash cryptocurrency. Compliance departments at certain financial institutions have interpreted the FinCEN and DOJ statements to mean that being associated with DCG indicates "high-risk activity that is indicative of possible criminal conduct . . . " We have learned that traditional bank account openings have been refused on the basis of a person's association with Dash-again, as a direct and express result of FinCEN's and DOJ's false characterization. These impacts are affecting all DCG members, to the extent employees and subcontractors of Dash have the option of receiving their salary in Dash cryptocurrency. Of course, as the recent news from Bittrex simply confirms, FinCEN's (and DOJ's) misinformed, off-the-cuff references to Dash as a money laundering risk in official U.S. government documents may lead to additional significant repercussions for DCG members, as mere association with a project deemed to support illicit purposes could (and, by all indications, likely will) lead to further unjustified blacklisting within the United States, and around the world.

5 Conclusion

DCG strongly objects to FinCEN's inclusion of Dash in the NPR as an AEC that poses a law enforcement and national security threat. It is unacceptable to reference Dash in this light, especially where we have-

– proactively reached out to FinCEN to describe how the Dash cryptocurrency works;

[11] Nasdaq, "Bittrex to Delist 'Privacy Coins' Monero, Dash and Zcash," Jan. 1, 2021, available at: `https://www.nasdaq.com/articles/bittrex-to-delist-privacy-coins-monero-dash-and-zcash-2021-01-01`; see also Bittrex, "Pending Market Removals 01/15/21," Jan. 1, 2021, available at: `https://bittrex.zendesk.com/hc/en-us/articles/360054393492-Pending-Market-Removals-01-15-21`

[12] Id.

- where reputable third parties (with whom we have no connection) have independently confirmed our points;
- where there is no evidence that Dash is actually used in illicit ways;
- where we have received no clarification from FinCEN as to why the agency believes Dash to be an AEC, and where it has never articulated a response to our fact-based arguments.

Meanwhile, we continue to suffer real (and possibly irreversible) harm as a result of the U.S. government's actions.

DCG is available to resolve any questions and is happy to continue to engage with FinCEN. But we respectfully ask you to act quickly. There is simply no justification for the U.S. government's continued behavior in labelling the Dash cryptocurrency an AEC. Until the definitional issue is resolved, please remove any and all references to Dash in the pending Rule (and in any materials surrounding it).