



## Comments of the Regulatory Action Center

Re: Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets

Docket ID: 85 FR 83840

January 7, 2021

The Regulatory Action Center at FreedomWorks Foundation is dedicated to educating Americans about the impact of government regulations on economic prosperity and individual liberty. FreedomWorks Foundation is committed to lowering the barrier between millions of FreedomWorks citizen activists and the rule-making process of government bureaus to which they are entitled to contribute.

---

On behalf of over 5.7 million activists nationwide, FreedomWorks Foundation appreciates the opportunity to offer these comments regarding the notice and request for comments on *Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets* (85 FR 83840). This notice seeks comment on the proposal to “require banks and money service businesses (‘MSBs’) to submit reports, keep records, and verify the identity of customers in relation to transactions involving convertible virtual currency.”

We take issue with the proposed rule for two separate, but equally important reasons. The first is a procedural concern, while the second is directed towards the content of the proposed rule. First of all, there is no justifiable reason for the Financial Crimes Enforcement Network (FinCEN) to rush this proposed regulation through at the midnight hour, and FinCEN’s decision to solicit a mere 15-day comment period is a blatant abuse of emergency powers. Secondly, requiring banks and MSB’s to provide identifying information for both hosted and unhosted wallets will, in effect, give federal regulators dangerous and unprecedented access to American’s financial data.

Before continuing, it is important to note that FinCEN’s reasoning behind the proposed rule is not entirely unfounded. The nature of cryptocurrencies as a theoretically untraceable, unregulated, and decentralized currency have always led to its use in illicit transactions. As FinCEN outlines in the rule, cryptocurrencies are used by malign actors for a myriad of malicious purposes. Most notably, crypto-ransomware attacks like WannaCry and its subsequent variants are growing in frequency and severity.<sup>1</sup>

---

<sup>1</sup> Whittaker, Zack. “Two years after WannaCry, a million computers remain at risk.” *Tech Crunch*. May 12, 2019. <https://techcrunch.com/2019/05/12/wannacry-two-years-on/>



However, federal regulators must be wary of missing the forest for the trees. As is too often the case, this proposed rule represents a drastic federal overreaction that threatens the future of cryptocurrencies. In their effort to clamp down on financial crime, it appears that FinCEN has failed to account for all the external costs of their proposed action. This proposal is simply the latest example of financial regulators abusing their authority under the Bank Secrecy Act in a blatant power grab.<sup>2</sup>

There is proof enough of this fact in the procedure by which FinCEN decided to propose this rule change. Citing “significant national security imperatives,” federal regulators used emergency powers to allow only 15 days of public comment, one quarter of the traditional 60 days. These emergency provisions are only supposed to be used for issues that offer a clear and present danger to national security that requires immediate federal action. Yet, in spite of the fact that there is no indication that cryptocurrency transactions are an immediate threat to our national security, FinCEN used these emergency powers to rush through the proposed rule.

To make matters worse, rather than propose this ruling at a reasonable time, FinCEN released the rule late on December 23rd, meaning the public comment period spanned across the Christmas and New Years holidays. There is no other way to read these actions other than disingenuous on the part of our financial regulators. If FinCEN’s intentions are genuine, they should have taken this proposed rule through the fair and open process that is statutorily required under 5 U.S. Code § 553 rather than using tricks and loopholes in an attempt to sneak it past the American public.

In addition to our serious objections to the process under which this proposed rule was promulgated, we are also opposed to much of the rule’s the content. The primary problem with the proposed rule is that it fails to account for the nuances between different types of coins and wallets. FinCEN’s blanket approach is at odds with the disparate world of cryptocurrencies.

For example, many cryptocurrencies such as Bitcoin utilize a public ledger that is recorded permanently in the blockchain. Under the current system, although the transaction ledger is public, the fact that a wallet user’s financial information is secured behind an encrypted wallet means that both personal information and transaction data are relatively secure. By attaching key identifiers to all private wallets, federal regulators are effectively mandating that

---

<sup>2</sup> Harper, Jim. “Questions about special regulation of cryptocurrency service providers.” *American Enterprise Institute*. January 4, 2021. <https://www.aei.org/technology-and-innovation/questions-about-special-regulation-of-cryptocurrency-service-providers/>



wallet providers remove all anonymity from cryptocurrencies. In doing so, FinCEN is creating the very real possibility of dangerous bulk financial data collection.

Mandating identifying information for both hosted and unhosted wallets has the potential to render many cryptocurrencies useless. Armed with both the user information for a particular crypto wallet and the publicly available ledger, both the federal government and savvy hackers could easily gain unprecedented access to American's financial information. This type of information would be practically impossible to collect absent the proposed rule, and many cryptocurrencies were designed specifically to minimize this possibility. In the wake of revelations about other bulk data collection by the intelligence community, granting federal regulators another tool to collect massive amounts of data on American citizens without a warrant is incredibly worrisome.<sup>3</sup>

Taken together, the gross overreach of the proposed rule and the process by which it was promulgated are justifiably concerning to a broad swath of stakeholders.<sup>4</sup> Pushing this regulation through at the last minute is a blatant power grab by financial regulators who have been antagonistic to the cryptocurrency industry from the very beginning. It is our hope that FinCEN will listen to the outpouring of public comments condemning this docket and retract this action in its entirety.

Respectfully submitted,

Luke Hogg  
Policy Analyst  
FreedomWorks Foundation

---

<sup>3</sup> Neidig, Harper. "Appeals court rules NSA's bulk phone data collection illegal." *The Hill*. September 2, 2020. <https://thehill.com/policy/national-security/514854-court-rules-nsas-bulk-phone-data-collection-illegal>

<sup>4</sup> Lopatto, Elizabeth. "Congratulations, the US got you cryptocurrency regulation for Christmas." *The Verge*. December 22, 2020. <https://www.theverge.com/2020/12/22/22195834/cryptocurrency-fincen-regulations-private-wallets>