Before the
FINANCIAL CRIMES ENFORCEMENT NETWORK
U.S. DEPARTMENT OF THE TREASURY
Washington, D.C. 20220

COMMENTS OF THE COMPETITIVE ENTERPRISE INSTITUTE

In the Matter of	)	
	)	
Financial Crimes Enforcement	)	FinCEN-2020-0020
Network (FinCEN)	)	RIN 1506-AB47
	)	
Proposed Rulemaking on	)	
"Requirements for Certain	)	
Transactions Involving Convertible	)	
Virtual Currency or Digital Assets"	)	

March 29, 2021

Ryan Nabil
John Berlau
COMPETITIVE ENTERPRISE INSTITUTE
1310 L Street NW, 7th Floor
Washington, DC 20005
(202) 331-1010

Introduction and CEI background

On behalf of the Competitive Enterprise Institute (CEI), we respectfully submit these comments in response to the Financial Crimes Enforcement Network's (FinCEN) notice of proposed rulemaking on covered cryptocurrency.[1] Founded in 1984, the Competitive Enterprise Institute is a non-profit research and advocacy organization that focuses on regulatory policy from a pro-market perspective. A strong focus of CEI is on removing regulations that inhibit choice, competition, and innovation, including financial innovation, as well as those that infringe on civil liberties

While expressing deserved admiration for America's courageous law enforcement personnel, CEI has voiced concern with laws and regulations enacted in the name of fighting crime that compromise law-abiding Americans' privacy and data security while doing little to catch bad actors. As such, CEI has long criticized aspects of the Bank Secrecy Act and pursuant regulations implemented by FinCEN that we believe are harmful to civil liberties and economic freedom. Over the decades, CEI has made common cause with progressive organizations, including the American Civil Liberties Union, to fight regulations that infringe on privacy rights and disproportionately affect marginalized Americans.[2] In 2000, CEI published the book *The Future of Financial Privacy*, which featured perspectives from an array of U.S. and European legal experts on policies affecting the security and confidentiality of financial data, including Bank Secrecy Act regulations.[3]

As FinCEN reexamines the current regulatory approaches to "convertible virtual currency" (CVCs) and "digital assets with legal tender status" (LTDA), it needs to address legitimate security and law enforcement concerns while

[1] Financial Crimes Enforcement Network (FinCEN), "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," 85 Federal Register 83840, December 23, 2020, https://www.federalregister.gov/documents/2021/01/28/2021-01918/requirements-for-certain-transactions-involving-convertible-virtual-currency-or-digital-assets#citation-1-p7352.

[2] John Berlau, "GSE Bailout Contains Fingerprint Registry," Competitive Enterprise Institute blog, July 23, 2008, https://cei.org/blog/gse-bailout-contains-fingerprint-registry/; Iain Murray, "ACLU Blast Federal Bank Regulators for Unconstitutional Power Grab," Competitive Enterprise Institute blog, October 27, 2016, https://cei.org/blog/aclu-blasts-federal-bank-regulators-for-unconstitutional-power-grab/.

[3] Competitive Enterprise Institute (CEI), *The Future of Financial Privacy* (Washington, DC: CEI, 2000), https://cei.org/studies/the-future-of-financial-privacy/.

maximizing economic freedom for virtual currency users.[4] Recently, FinCEN proposed a new rule, which would i) mandate banks and money service businesses (MSBs) to report certain CVC and LTDA transactions worth over $10,000 and ii) require banks and MSBs to store customer and counterparty information on covered CVC and LTDA transactions worth $3,000 or more.[5] If implemented, these two requirements will apply to "transactions above certain thresholds involving CVC/LTDA wallets not hosted by a financial institution (also known as 'unhosted wallets') or CVC/LTDA wallets hosted by a financial institution in certain jurisdictions identified by FinCEN."[6] We argue that the costs of the proposed regulations—in terms of compromised privacy and data security for lawful users of cryptocurrency as well as barriers to entry for new MSBs and developers of digital assets—vastly exceed any potential benefits. For these reasons, FinCEN should not implement the rule.

More specifically, we express five concerns about FinCEN's proposed rulemaking. First, as part of the Anti-Money Laundering Act (AMLA) passed on January 1, 2021, Congress instructed the Treasury Department to examine the effectiveness and perform a cost-benefit analysis of the Currency Transaction Report (CTR) and the Suspicious Activity Report (SAR) for covered transactions.[7] Before mandating similar requirements for covered cryptocurrency transactions, Treasury should complete its study on the costs and effectiveness of existing reporting requirements. Once this report is published, FinCEN should review the proposed rule and reopen the notice-and-comment period to seek further public comments.

Second, the proposed rule goes beyond the Bank Secrecy Act's legislative intent and raises strong Fourth Amendment concerns by allowing the U.S. government to obtain a record of *all* transactions associated with a covered private

[4] FinCEN, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," 85 Federal Register 83840.

[5] FinCEN, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets."

[6] David Zaslowsky, "FinCEN Introduces Proposed Crypto Reporting Requirements," Baker McKenzie Blog, December 22, 2020, https://blockchain.bakermckenzie.com/2020/12/22/fincen-introduces-proposed-crypto-reporting-requirements/; FinCEN, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets."

[7] Public Law No.: 116-283, §§ 6001-6511.

wallet, as well as those of its transacting counterparties, without obtaining a warrant.[8]

Third, the proposed rule would create substantial cybersecurity risks by storing sensitive personal information in a central government database. Such a database would make for a tempting target for malicious actors seeking such financial records to conduct surveillance of American citizens.[9] Given the growing number of data breaches in federal agencies, FinCEN should be careful not to introduce additional cybersecurity risks by mandating new reporting requirements.[10]

Fourth, FinCEN's proposed rule will create significant regulatory burdens for financial intermediaries, as they may be unable to determine whether the recipient wallets are "hosted" by financial institutions.[11] Consequently, banks and MSBs will likely have to focus compliance efforts on reporting a high volume of transactions instead of identifying and reporting suspicious transactions. In the long run, if the compliance costs and cybersecurity concerns become too high, consumers and MSBs might choose more business-friendly foreign jurisdictions for cryptocurrency transactions. Such a development would reduce law enforcement's access to potential data as more transactions move beyond U.S. jurisdiction.[12]

---

[8] Electronic Frontier Foundation (EFF), "Comments to the Financial Crimes Enforcement Network (FinCEN) on Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," January 4, 2021, https://www.eff.org/document/2021-01-04-eff-comments-fincen.

[9] Blockchain Association, "Comments on the Financial Crimes Enforcement Network's Notice of Proposed Rulemaking on 'Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets,'" January 4, 2021, 8, https://theblockchainassociation.org/wp-content/uploads/2021/01/BA-Response-to-FinCEN-2020-0020.pdf.

[10] For a detailed discussion, see "Section III: The proposed rule will increase cybersecurity risks."

[11] Edward So and Jeremy Kuester, "FinCEN's proposed regulation of virtual assets," White & Case, January 5, 2021, https://www.whitecase.com/publications/alert/fincens-proposed-regulation-virtual-assets.

[12] EFF, "Comments to FinCEN"; Federico Paesano, "Will new FinCEN rules drive cryptocurrency users underground?", Basel Institute on Governance, January 7, 2021, https://baselgovernance.org/blog/will-new-fincen-rules-drive-cryptocurrency-users-underground.

Finally, by increasing regulatory costs, the proposed rule will slow down smart contracts and other blockchain-based technological innovations.[13] Due to these reasons, we urge FinCEN not to implement the proposed rule.

I. FinCEN's rulemaking timeline raises procedural concerns.

FinCEN's timeline to the proposed rulemaking suggests an intent to promote midnight rulemaking without allowing sufficient time to consider how the rules will affect MSB operations. On December 18, 2020, FinCEN announced a two-week window for comments—including the holidays in late December—instead of the 60-day notice-and-comment requirements as required under the Administrative Procedure Act (APA).[14] More specifically, FinCEN argued that the proposed rulemaking "is exempt from the APA's notice-and-comment requirements because it involves a 'foreign affairs function' and because it 'advances foreign policy and national security interests of the United States, using a statute that was designed in part for that purpose.'"[15] However, "[f]or the [foreign affairs exemption] to apply," FinCEN would need to demonstrate that "the public rulemaking provisions should provoke definitely undesirable international consequences"—which FinCEN failed to establish clearly.[16]

Two factors further weaken FinCEN's national security argument to waive the 60-day notice-and-comment-requirement. First, like most banking transactions, many cryptocurrency transactions between hosted and unhosted wallets include only domestic participants, limiting their potential effect on national security and foreign affairs function of the United States. Second, FinCEN has adopted no such reporting rules for transactions between two privately hosted wallets that bypass MSBs altogether, which would arguably pose a more significant security concern. Consequently, many industry participants and MSBs argued that FinCEN used a shorter period to bypass further scrutiny of its

[13] EFF, "Comments to FinCEN," 8–10; Blockchain Association, "Comments on FinCEN Rulemaking," 9.

[14] U.S. Treasury, Financial Crimes Enforcement Network (FinCEN), "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," RIN 1506-AB47, 1, https://public-inspection.federalregister.gov/2020-28437.pdf.

[15] Square Inc., "Square, Inc.'s Federal Comment Letter Regarding FinCEN's Proposed Rulemaking on Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," January 4, 2021, https://squareup.com/us/en/press/fincen-letter; FinCEN, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets."

[16] Square Inc., "Square, Inc.'s Federal Comment Letter."

proposed rulemaking.[17] Such concerns are reflected by the fact that over 7,000 participants initially filed comments with FinCEN, with many of these comments pointing out the proposed rule's rushed timeline.[18] As a result, FinCEN extended the deadline for filing comments twice, and the final deadline, as of filing this comment, remains March 29, 2021.[19]

Although this extension of the deadline to file comments is a step in the right direction, it will likely be insufficient in light of recent developments. As noted, under the Anti-Money Laundering Act (AMLA), which was passed on January 1, 2021, Congress instructed the Treasury Department to examine the effectiveness and perform a cost-benefit analysis of the Currency Transaction Report (CTR) and the Suspicious Activity Report (SAR).[20] Based on this report, Congress seeks to determine whether the regulatory burden associated with these two requirements exceeds the benefits of reporting such information.[21] Before these two reporting requirements are extended to MSBs for covered transactions involving un-hosted wallets, Treasury should first complete its study of the effects of CTR and SAR on covered transactions. Once this study is finished, Congress and Treasury will have a clearer idea about which regulations can help to effectively combat financial crimes and which ones create an unnecessary regulatory burden for financial institutions. For these reasons, FinCEN should review the proposed rule in light of the report's finding and then reopen the notice-and-comment-period to seek public comments.

II. The proposed rule exceeds FinCEN's authority under the BSA and raises Fourth Amendment concerns.

[17] Financial Crimes Enforcement Network (FinCEN), "FinCEN Extends Comment Period for Rule Aimed at Closing Anti-Money Laundering Regulatory Gaps for Certain Convertible Virtual Currency and Digital Asset Transactions," January 14, 2021, https://www.fincen.gov/news/news-releases/fincen-extends-comment-period-rule-aimed-closing-anti-money-laundering; FinCEN, "FinCEN Extends Reopened Comment Period for Proposed Rulemaking on Certain Convertible Virtual Currency and Digital Asset Transactions," U.S. Treasury, January 26, 2021, https://www.fincen.gov/news/news-releases/fincen-extends-reopened-comment-period-proposed-rulemaking-certain-convertible.

[18] Nikilesh De and Kevin Reynolds, "FinCEN Extends Comment Period for Controversial Crypto Wallet Rule," Coindesk, January 14, 2021, https://www.coindesk.com/fincen-extends-comment-period-for-controversial-crypto-wallet-rule-by-15-days.

[19] FinCEN, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," 86 Federal Register 7352, January 1, 2021.

[20] Public Law No.: 116-283, §§ 6001-6511.

[21] Public Law No.: 116-283, §§ 6001-6511.

By implementing the proposed rule, FinCEN claims to bring the reporting requirements for cryptocurrencies in line with cash-based transactions under the Bank Secrecy Act (BSA). Under the BSA, financial institutions are required to file a Currency Transaction Report (CTR) within 15 calendar days of a cash transaction of $10,000 or greater.[22] Likewise, financial institutions must keep records of customer information for money transfers of "$3,000 or more, regardless of the method of payment."[23]

However, under existing regulations, financial intermediaries are not required to report customer information about transactions involving an unhosted wallet if the amount is less than $10,000. Likewise, banks and MSBs are also not required to keep records of a transaction involving an unhosted wallet if the transaction is worth less than $3,000. By mandating reporting and recording requirements for these two types of transactions, FinCEN claims to create equivalence between cash and virtual currency transactions. According to FinCEN, equivalence is essential since CVC and LTDA should be treated as "monetary instruments" under the BSA.[24]

FinCEN proposes two new requirements to create "equivalent" reporting standards for transactions in CVC and LTDA. These two requirements will apply to "transactions above certain thresholds involving CVC/LTDA wallets not hosted by a financial institution (also known as 'unhosted wallets') or CVC/LTDA wallets hosted by a financial institution in certain jurisdictions identified by FinCEN" (known as "otherwise covered wallets").[25]

---

[22] 31 Code of Federal Regulation (CFR) §1010.310-314; FinCEN, "Bank Secrecy Act Requirements," accessed March 26, 2021, https://www.fincen.gov/sites/default/files/shared/bsa_quickrefguide.pdf.

[23] FinCEN, "Bank Secrecy Act Requirements," U.S. Treasury, accessed March 24, 2021, https://www.fincen.gov/sites/default/files/shared/bsa_quickrefguide.pdf; 31 CFR §1010.410, §1010.415.

[24] FinCEN argues that CVC and LTDA should be treated as "monetary instruments" because "they constitute 'similar material' to instruments described in 31 U.S.C 5312(a)(3)(B) ('coins and currency of a foreign country, travelers' checks, bearer negotiable instruments, bearer investment securities, bearer securities, [and] stock on which title is passed on delivery…')" (FinCEN, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," 85 Federal Register 83840, December 23, 2020).

[25] David Zaslowsky, "FinCEN Introduces Proposed Crypto Reporting Requirements," BakerMcKenzie Blog, December 22, 2020, https://blockchain.bakermckenzie.com/2020/12/22/fincen-introduces-proposed-crypto-reporting-requirements/. More specifically, "FinCEN is proposing to define otherwise covered wallets as those wallets that are held at a financial institution that is not subject to the BSA and is located in a foreign jurisdiction identified by FinCEN on a List of Foreign Jurisdictions Subject to 31 CFR 1010.316

First, for transactions greater than $10,000, the proposed rule would require financial intermediaries "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), and to verify the identity of their customer, if a counterparty to the transaction is using an unhosted or otherwise covered wallet and the transaction is greater than $10,000."[26]

Second, "the proposed rule would require banks and MSBs to keep records of a customer's CVC or LTDA transaction and counterparty, including verifying the identity of their customer if a counterparty is using an unhosted or otherwise covered wallet and the transaction is greater than $3,000."[27]

By implementing these two mandates, FinCEN claims to make cryptocurrency transaction reporting requirements consistent with CTR requirements for cash transactions. The CTR requirement creates a record of cash transactions, pursuant to the rationale that such record is essential given the ephemeral and anonymous nature of cash.[28] By imposing CTR requirements on banks and MSBs, FinCEN and the Internal Revenue Service (IRS) gain the ability to create a central database of reported cash transactions of $10,000 and higher.[29]

Although the CTR requirements apply to cash-based transactions, extending them to cryptocurrency transactions would be a mistake for several reasons. First, most leading cryptocurrencies, such as Bitcoin and Ethereum, are "unshielded," which means that transactions in those currencies are permanently recorded and searchable on a publicly available ledger.[30]

Reporting and 31 CFR 1010.410(g) Recordkeeping (the 'Foreign Jurisdictions List'). Initially, FinCEN is proposing that the Foreign Jurisdictions List be comprised of jurisdictions designated by FinCEN as jurisdictions of primary money laundering concern (i.e. Burma, Iran, and North Korea)." (FinCEN, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," 85 Federal Register 83840, December 23, 2020).

[26] FinCEN, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets." The reporting requirement also applies if "the transaction is greater than $10,000 (or the transaction is one of multiple CVC transactions involving such counterparty wallets and the customer flowing through the bank or MSB within a 24-hour period that aggregate to value in or value out of greater than $10,000)" (FinCEN, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets").

[27] FinCEN, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets."

[28] 31 CFR §1010.310-314.

[29] 31 CFR §1010.330 (1) (ii).

[30] In contrast, privacy-oriented cryptocurrencies can offer both "shielded" and "unshielded" transactions (Investopedia, 2021). For example, "as of January 2020, 15.5 percent of ZCash

Second, law enforcement agencies already can access financial records for investigative purposes without mandating a CTR-like requirement for "unshielded" cryptocurrency transactions. They have access to analytic tools, such as Chainalysis and Coinpath, which provide them with the means to search for "unshielded" cryptocurrency transactions recorded on the blockchain.[31] Furthermore, following the Fifth Circuit's *Gratkowski* decision in 2020, law enforcement agencies may use analytic software to search publicly available cryptocurrency records without a warrant.[32] Based on such information, they can subpoena the financial intermediaries for the names and addresses of a specific wallet.[33] Although the proposed rule might be appropriate for privacy-oriented cryptocurrencies and "shielded" transactions, there is no reason to impose the same requirement on "unshielded" cryptocurrency transactions.

Furthermore, the proposed rule will undermine American consumers' reasonable expectation of privacy for cryptocurrency transactions. "Unshielded" cryptocurrency transactions are permanently recorded on the blockchain, and can be viewed by the public.[34] However, due to the blockchain's anonymized nature,

---

transactions were shielded," while the remaining 84.5 percent of ZCash transactions were "unshielded" (Silfverstein et al., 2020; ZChain, 2020). In contrast, all Monero transactions are "shielded" by default, meaning that they are not recorded on a public blockchain (Monero, 2021). As a result, Monero transactions are much harder to trace than transactions in leading cryptocurrencies such as Bitcoin and Ethereum (Monero, 2021). See Investopedia, "6 Private Cryptocurrencies," updated January 5, 2021, https://www.investopedia.com/tech/five-most-private-cryptocurrencies/; Erin Silfversten, Marina Favaro, Linda Slapakova, Sasha Ishikawa, James Liu, and Adrian Salas, *Exploring the Use of Zcash Cryptocurrency for Illicit or Criminal Purposes* (Cambridge: RAND Corporation, 2020), https://www.rand.org/content/dam/rand/pubs/research_reports/RR4400/RR4418/RAND_RR4418.pdf; ZChain, "Total value exchanged over a given pool type," Zchain Explorer, accessed February 11, 2020, https://explorer.zcha.in/statistics/values; Jack Martin, "Zcash Fully Shielded Transactions Jump 70% to New Record in April," May 4, 2020, https://cointelegraph.com/news/zcash-fully-shielded-transactions-jump-70-to-new-record-in-april; Monero, "What is Monero (XMR)?", n.d., accessed March 24, 2021, https://www.getmonero.org/get-started/what-is-monero/.

[31] Bitquery, "Best Blockchain Analysis Tools and How They Work?", August 18, 2020, https://bitquery.io/blog/best-blockchain-analysis-tools-and-software.

[32] *United States v. Gratkowski,* 964 F.3d 307 (5th Cir. 2020); Richard Johnson, Margaret Lyle, Mark Rasmussen, and Shamoli Shipchandler, "No Search Warrant Required for Records of Bitcoin Transactions, the Fifth Circuit Holds," JD Supra, August 12, 2020, https://www.jdsupra.com/legalnews/no-search-warrant-required-for-records-39560/.

[33] Johnson et al., "No Search Warrant Required for Records of Bitcoin Transactions, the Fifth Circuit Holds."

[34] Kevin Werbach, "Trust, but Verify: Why the Blockchain needs the Law," *Berkeley Technology Law Journal* 33 (487), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2844409; EFF, "Comments to FinCEN."

other users cannot attribute those transactions to a specific person unless they know the name and address of the wallet used for the transactions. Consequently, the names and addresses of a wallet are potentially the most sensitive information in cryptocurrency transactions. Once the government—or malign actors—match the name and address with a specific wallet, they can view a person's entire financial history associated with that wallet.

As a result, the proposed rule poses at least three obstacles for consumers seeking privacy and data security. First, when a financial intermediary reports the personal information associated with a wallet for a transaction over $10,000, the government will gain access to that person's entire financial history related to the wallet.[35] That includes transactions far below $10,000, which goes beyond the legislative intent for CTRs under the BSA.[36]

Second, the recordkeeping requirement for cryptocurrency transactions over $3,000 means that financial intermediaries will have access to the person's entire financial history associated with that wallet.[37] Such records will include transactions well below even the $3,000 threshold.[38]

Finally, the proposed rule will require financial intermediaries to report the personal information of their customers' counterparties, in addition to that of the customers.[39] That means that the financial intermediaries and the government would gain access to the entire financial history of counterparty entities without receiving consent to such data collection.

For the reasons stated above, the proposed rule goes far beyond the CTR reporting requirement as intended under the BSA.[40] Instead of creating equivalent

---

[35] FinCEN, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," 85 Federal Register 83840, December 23, 2020.

[36] EFF, "Comments to FinCEN," 5.

[37] FinCEN, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," 85 Federal Register 83840, December 23, 2020.

[38] EFF, "Comments to FinCEN," 5.

[39] FinCEN, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," 85 Federal Register 83840, December 23, 2020.

[40] Other commentators have made similar points. For example, see Fidelity Digital Assets, "Comment Letter on Proposed Rule on Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," January 4, 2021, https://beta.regulations.gov/comment/FINCEN-2020-0020-6014; Brian R. Michael, Daniel R. Kahan, Matthew B. Hanson, Shaswat K. Das, Jacob Gerber, and Brendon Walsh, "Pumping the Brakes: FinCEN Reopens Comment Period for Controversial Crypto Reporting & Recordkeeping Rules," King & Spalding, January 15, 2021, https://www.kslaw.com/news-and-insights/pumping-

reporting requirements between cash and cryptocurrency transactions, this rule would be tantamount to the government gaining information about a person's entire cash transaction history without a warrant.[41]

Consequently, the proposed rule raises significant concerns about the Fourth Amendment's constitutional protections against "unreasonable searches and seizures" in cryptocurrency transactions. [42] The traditional government defense for record-keeping and reporting requirements known as the "third-party doctrine," which rests on the premise that consumers voluntarily give the information in question to a bank or other business, may not hold water with the courts given the extraordinary reach of this rule. The Supreme Court has signaled in recent cases that the "third-party doctrine" has its limits, particularly when consumers expect that the data will be kept private. As the Court stated in *Carpenter v. United States*, "this Court has never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy."[43] Therefore, even if other federal circuits and the Supreme Court uphold the Fifth Circuit's *Gratkowski* ruling that access to public blockchain data does not require a warrant, this rule's demand for routine access to sensitive personal data about cryptocurrency users' identities may not survive Fourth Amendment scrutiny.[44]

In response to criticisms, the proponents of this rule might point to virtual currencies' potential use in money laundering and terrorist financing.[45] Despite these legitimate concerns, economic evidence suggests that policymakers overestimate cryptocurrency's illegal use.[46] In 2019, "[i]llicit purchases accounted

---

the-brakes-fincen-reopens-comment-period-for-controversial-crypto-reporting-recordkeeping-rules#_ednref21.

[41] Blockchain Association, "Comments on FinCEN's Proposed Rulemaking."

[42] U.S. Const. amend. IV; Blockchain Association, "Comments on FinCEN's Proposed Rulemaking"; 585 U.S. 16-402 138 S. Ct. 2206; 201 L. Ed. 2d 507.

[43] *Carpenter v. United States*, 138 S. Ct. 2206 (2018). See also *Riley v. California*, 134 S. Ct. 2473 (2014).

[44] *United States v. Gratkowski,* 964 F.3d 307 (5th Cir. 2020); 138 S. Ct. 2206 (2018).

[45] Marshall Hayner, "FinCEN's new rule will protect Americans and accelerate cryptocurrency's adoption," *The Hill*, December 28, 2020, https://thehill.com/opinion/finance/531811-fincens-new-rule-will-protect-americans-and-accelerate-cryptocurrencys.

[46] Ryan Nabil, "Why a Biden Administration Attack on Cryptocurrencies Would Be a Mistake," *The National Interest*, February 1, 2021, https://nationalinterest.org/blog/buzz/why-

for less than 0.5 percent of all transactions associated with Bitcoin, the most popular virtual currency, according to data from Elliptic, a blockchain analysis company."[47] Furthermore, more than 70 percent of Bitcoin transferred into unhosted wallets reportedly stay in those wallets instead of being transferred to another wallet.[48] That suggests that unhosted wallets (at least for Bitcoin) are used primarily as a store of wealth rather than as a conduit for money laundering and other criminal purposes.[49] Nonetheless, it should be recognized that illegal activity using "shielded" transactions might be more difficult for law enforcement agencies to trace. That is why FinCEN should adopt different regulatory standards for "shielded" and "unshielded" cryptocurrency transactions and respect consumer privacy in "unshielded" cryptocurrency transactions.

Given this context, FinCEN should recognize the legitimate reasons why individual customers might seek privacy in financial transactions. As the Electronic Frontier Foundation points out, consumers have historically used cash to protect personal information regarding financial, political, and religious activities.[50] The same desire for privacy also motivates some consumers to use virtual currencies and digital assets instead of non-cash monetary instruments.[51]

Such concerns are especially significant in countries with authoritarian regimes, where cryptocurrency transactions can help individuals evade government surveillance.[52] Pro-democracy protestors in Hong Kong and Ukraine have reportedly used cash to avoid being detected by authorities while partaking

---

biden-administration-attack-cryptocurrencies-would-be-mistake-177411; Silfversten et al, *Exploring the Use of Zcash Cryptocurrency for Illicit or Criminal Purposes*.

[47] Nabil, "Why a Biden Administration Attack on Cryptocurrencies Would Be a Mistake". For more information, see Elliptic, "Bitcoin Money Laundering: How Criminals Use Crypto," September 18, 2019, https://www.elliptic.co/blog/bitcoin-money-laundering; Tom Robinson and Yaya Fanusie, *An Analysis of Illicit Flows into Digital Currency Services* (Elliptic and the Foundation for the Defense of Democracies, January 12, 2018), https://info.elliptic.co/whitepaper-fdd-bitcoin-laundering.

[48] Federico Paesano, "Will new FinCEN rules drive cryptocurrency users underground?", Basel Institute on Governance, January 7, 2021, https://baselgovernance.org/blog/will-new-fincen-rules-drive-cryptocurrency-users-underground.

[49] Paesano, "Will new FinCEN rules drive cryptocurrency users underground?".

[50] EFF, "Comments to FinCEN," 3.

[51] EFF, "Comments to FinCEN," 3; Anna Baydakova, "Bitcoin Dissidents: Those Who Need It Most," Coindesk, December 8, 2021, updated December 30, 2020, https://www.coindesk.com/bitcoin-protesters-most-influential-2020.

[52] EFF, "Comments to FinCEN," 3; Baydakova, "Bitcoin Dissidents."

in such activities.[53] Like cash, cryptocurrency can offer activists and organizations a level of privacy and anonymity that they would not get from other non-cash monetary instruments. Although the exact data on this phenomenon remains limited due to the anonymous nature of blockchain and the need for privacy, pro-democracy organizations such as the Hong Kong Free Press receive donations in cryptocurrencies.[54] Cryptocurrency-based donations would allow such groups in Hong Kong and Russia to continue their activities even if their respective governments were to arrest activists and freeze their bank accounts.[55] Therefore, it is no wonder that authoritarian countries—such as China[56] and Russia[57]—have adopted a restrictive approach towards cryptocurrencies. Instead of adopting policies characteristic of authoritarian regimes, the United States should minimize government surveillance and ensure privacy for U.S. citizens and customers of U.S.-based financial intermediaries.[58]

III. The proposed rule will increase cybersecurity risks.

[53] EFF, "Comments to FinCEN," 3; Baydakova, "Bitcoin Dissidents."

[54] EFF, "Comments to FinCEN," 3; Baydakova, "Bitcoin Dissidents."

[55] Baydakova, "Bitcoin Dissidents."

[56] The Chinese government "does not recognize cryptocurrencies as legal tender and the banking system is not accepting cryptocurrencies or providing relative services. The government has taken a series of regulatory measures to crackdown on activities related to cryptocurrencies for the purposes of investor protection and financial risk prevention." Library of Congress, "Regulation of Cryptocurrency: China," last updated December 30, 2020, https://www.loc.gov/law/help/cryptocurrency/china.php/. Tthe People's Bank of China, the Chinese central bank, has launched "the digital renminbi" to compete with foreign cryptocurrencies. James Kynge and Sun Yu, "Virtual control: the agenda behind China's new digital currency," *Financial Times*, February 17, 2021, https://www.ft.com/content/7511809e-827e-4526-81ad-ae83f405f623; Caixin, "社论丨不必急推数字人民币" ["Editorial: For China, Getting the Digital Yuan Right is More Important than Getting It First"], September 8, 2020, https://www.caixinglobal.com/2020-09-08/editorial-for-china-getting-the-digital-yuan-right-is-more-important-than-getting-it-first-101602509.html.

[57] Cryptocurrency transactions are banned in Russia pursuant to Federal Law No. 259-FZ, art.1, §§ 1, 2 & 3. See Российсая Газета [Rossiksya Gazeta], "Федеральный закон от 31 июля 2020 г. N 259-ФЗ 'О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации'" ["Federal Law of July 31, 2020 N 259-FZ 'On digital financial assets, digital currency and on amendments to certain legislative acts of the Russian Federation'"], August 6, 2020, https://perma.cc/5KZV-XDDN.

[58] The Blockchain Association makes a similar point: "Totally eliminating financial privacy for U.S. citizens just because they choose to use digital currency is not an acceptable or reasonable response to concerns about illicit financial activity. And it is certainly not a mere reporting requirement that should be imposed hastily and without express statutory authorization" (Blockchain Association, "Comments on FinCEN's Proposed Rulemaking," 8).

FinCEN's proposed regulation presupposes that personally identifiable data—which can reveal a person's entire cryptocurrency transaction history —can be safely stored with FinCEN and the IRS. However, growing evidence suggests that government databases are increasingly risky for storing sensitive data of MSB customers and their counterparties. In the last few years, the U.S. government and its agencies have been subject to a growing number of cyberattacks.[59] In 2015, an estimated 18 million personal records of current, former, and prospective federal employees were affected by a data breach at the Office of Personnel Management (OPM). [60] Further investigations revealed that Chinese intelligence sources allegedly gained access to over 22 million security-clearance files and over five million fingerprints due to this hack.[61] Many experts believe such attacks comprise growing foreign efforts at compiling databases on past and current federal employees, which could be used for nefarious purposes in the future.[62]

Even the National Security Agency (NSA)—arguably the federal agency with the best cybersecurity expertise—has proved ineffective against cyberattacks.[63] As *The New York Times* reported in June 2019, Chinese, Russian, and North Korean intelligence agencies gained access to the NSA's cyberweapons and tools and then deployed them in cyberoperations in Britain, Europe, and Asia.[64] Likewise, a cyberattack against the Customs and Border Patrol led to the exposure of license plate and traveler images of around 100,000 travelers, which

[59] Center for Strategic and International Studies, "Significant Cyber Incidents," accessed March 25, 2021, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

[60] Evan Perez and Shimon Prokupecz, "First on CNN: U.S. data hack may be 4 times larger than the government originally said," CNN, June 23, 2015, https://www.cnn.com/2015/06/22/politics/opm-hack-18-milliion/index.html.

[61] David E. Sanger, "Russian Hackers Broke into Federal Agencies, U.S. Officials Suspect," *New York Times*, updated February 9, 2021, https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html.

[62] Kevin Kiptak, Theodore Schleider, and Jim Sciutto, "China might be building vast database of federal worker info, experts say," CNN, updated June 5, 2015, https://www.cnn.com/2015/06/04/politics/federal-agency-hacked-personnel-management/.

[63] Matthew Gault, "The U.S. Government Is Utterly Inept at Keeping Your Data Secure," The New Republic, June 12, 2019, https://newrepublic.com/article/154167/government-nsa-inept-protecting-cyber-data-whatsapp.

[64] Nicole Perlroth, David E. Sanger and Scott Shane, "How Chinese Spies Got the N.S.A.'s Hacking Tools, and Used Them for Attacks," *New York Times*, May 6, 2019, https://www.nytimes.com/2019/05/06/us/politics/china-hacking-cyber.html.

were later made available for download on the dark web.[65] More recently, as the *Times reports*, in December 2020, "a Russian intelligence agency, according to federal and private experts—broke into a range of key government networks, including in the Treasury and Commerce Departments, and had free access to their email systems."[66]

These examples point to significant vulnerabilities in the U.S. government's storage of sensitive data. If FinCEN were to implement its proposed rule, FinCEN and the IRS would create a centralized database that could provide access to the cryptocurrency financial records of virtually all Americans with a private wallet (and those of their counterparties with a hosted wallet). As noted, that would make the FinCEN/IRS database a tempting target for malicious actors seeking such data to conduct surveillance of American citizens and potentially blackmail them.[67] As the Blockchain Association notes, "FinCEN itself has acknowledged that the unauthorized disclosure of private financial information '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.'"[68] Therefore, FinCEN should be careful not to introduce additional cybersecurity risks by creating a centralized database of Americans with a "self-hosted" wallet and their business partners.

Although a potential cyberattack on an individual financial institution will be much less consequential than an attack against the Treasury or the IRS, FinCEN should pay attention to the growing cybersecurity risks that these institutions face. Like federal agencies, financial institutions have become an important target for malicious actors.[69] Growing evidence suggests that attacks

---

[65] Thomas Claburn, "Maker of US border's license-plate scanning tech ransacked by hacker, blueprints and files dumped online," *The Register*, May 23, 2019, https://www.theregister.com/2019/05/23/perceptics_hacked_license_plate_recognition/; Gault, "The U.S. Government Is Utterly Inept at Keeping Your Data Secure."

[66] Sanger, "Russian Hackers Broke into Federal Agencies, U.S. Officials Suspect."

[67] Blockchain Association, "Comments on FinCEN's Proposed Rulemaking", 8.

[68] Blockchain Association, "Comments on FinCEN's Proposed Rulemaking", 8; FinCEN, "Statement Regarding Unlawfully Disclosed Suspicious Activity Reports," September 1, 2020, https://www.fincen.gov/news/news-releases/statement-fincen-regarding-unlawfully-disclosed-suspicious-activity-reports.

[69] CSIS, "Significant Cyber Incidents"; VMWare Carbon Black, "Modern Bank Heists' Threat Report from VMware Carbon Black Finds Dramatic Increase in Cyberattacks Against Financial Institutions Amid COVID-19," May 14, 2021, https://www.carbonblack.com/press-releases/modern-bank-heists-threat-report-from-vmware-carbon-black-finds-dramatic-increase-in-cyberattacks-against-financial-institutions-amid-covid-19/.

against banks and MSBs are likely to increase as the impact of the Covid-19 crisis accelerates the digitization of the U.S. and global economies.[70] According to VMWare Carbon Black, a cloud security provider, cyberattacks against financial institutions increased by 238 percent between February and April 2020 alone.[71] Such trends are a crucial reason why FinCEN should be concerned about potential cybersecurity attacks against MSBs to gain sensitive information.[72] Therefore, FinCEN should be careful not to introduce additional cybersecurity risks by mandating financial institutions to store sensitive information about their clients and their counterparties.

IV. The proposed rule will create high regulatory costs and reduce law enforcement's access to high-value data.

FinCEN's proposed reporting and recordkeeping requirements will create significant technical problems and compliance costs for banks and MSBs. Under the proposed regulation, banks and financial institutions would have to verify, store, and report personal information of clients and their counterparties if either of the two parties uses an "unhosted wallet."[73] However, due to the anonymous nature of cryptocurrency transactions, banks and MSBs do not currently possess the technical means to verify whether the counterparty has an "unhosted wallet."[74] To comply with the rule, financial intermediaries would need to verify and record personal information for *all* transactions over $3,000 and report such information for *all* transactions over $10,000.[75]

As a result, the proposed rule might be counterproductive in detecting criminal activity and money laundering by financial intermediaries and law enforcement agencies. In the short term, banks and MSBs will likely have to focus compliance efforts on reporting a high volume of transactions instead of identifying and reporting potentially suspicious transactions. However, such high-volume data will be of limited value for law enforcement, because records of

---

[70] Phil Muncaster, "Attacks on Banks Spike 238% During COVID19 Crisis," Info Security, May 15, 2020, https://www.infosecurity-magazine.com/news/attacks-on-banks-spike-238-during/.

[71] Muncaster, "Attacks on Banks Spike 238% During COVID19 Crisis."

[72] Blockchain Association, "Comments on FinCEN's Proposed Rulemaking," 8.

[73] FinCEN, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," 85 Federal Register 83840, December 23, 2020.

[74] Blockchain Association, "Comments on FinCEN's Proposed Rulemaking," 5-7.

[75] FinCEN, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," 85 Federal Register 83840, December 23, 2020.

unshielded cryptocurrency transactions are already available to law enforcement officials through blockchain analysis software.[76]

In the long term, FinCEN's proposed rule might decrease the quantity of data available to law enforcement and national security agencies for several reasons. First, if the proposed rule's compliance costs and cybersecurity risks are too high, financial intermediaries might scale down or end their cryptocurrency offerings.

Alternatively, financial institutions might decide to offer cryptocurrency payments in countries with a friendlier regulatory environment. Likewise, due to the potential privacy concerns and cybersecurity risks, individual consumers also might choose MSBs in safer jurisdictions without mandatory data retention and reporting policies.[77]

Finally, instead of relying on a financial intermediary, cryptocurrency participants can transfer money directly from one un-hosted wallet to another un-hosted wallet.[78] Because such transactions fall outside the scope of the proposed rule, it would allow market participants to bypass FinCEN's proposed reporting requirements.[79] As a result, these developments can significantly reduce the volume of cryptocurrency data that U.S. law enforcement agencies can access without a warrant.[80]

V. The proposed rule will undermine long-term U.S. economic competitiveness and innovation.

U.S. companies have made significant progress in digital and cryptocurrency innovation over the past decade.[81] That has allowed the United States to regain its competitive edge in financial technology—(FinTech) vis-à-vis

[76] Bitquery, "Best Blockchain Analysis Tools and How They Work?" August 18, 2020, https://bitquery.io/blog/best-blockchain-analysis-tools-and-software; *United States v. Gratkowski,* 964 F.3d 307 (5th Cir. 2020); Johnson et al., "No Search Warrant Required for Records of Bitcoin Transactions."

[77] See Sections III and IV for a longer discussion.

[78] Blockchain Association, "Comments on FinCEN's Proposed Rulemaking," 7.

[79] Blockchain Association, "Comments on FinCEN's Proposed Rulemaking," 7.

[80] Blockchain Association, "Comments on FinCEN's Proposed Rulemaking," 7.

[81] *The Economist*, "America used to be behind on digital payments. Not any more," March 20, 2021, https://www.economist.com/finance-and-economics/2021/03/20/america-used-to-be-behind-on-digital-payments-not-any-more.

its Asian and European competitors.[82] Notwithstanding such progress, FinCEN's proposed rule can harm America's economic competitiveness in digital payments. The two requirements will result in a significant regulatory burden for banks and MSBs and create considerable cybersecurity risks.[83] If banks and MSBs find the regulatory burden too high, they might eventually seek alternative jurisdictions with a more business-friendly regulatory environment. That is especially likely if a large-scale cyber-operation—such as the SolarWinds attack—target the U.S. governments and expose the personal financial transaction history of U.S.-based customers and their counterparties.[84] Given the growing challenges to U.S. cybersecurity and an increasing number of attacks against federal agencies and the private sector, FinCEN should be careful not to introduce additional cybersecurity risks by implementing its proposed rulemaking.[85]

Finally, the proposed rule can also hinder the development of future innovations that depend on blockchain technology.[86] FinCEN's notice of proposed rulemaking does not provide a precise definition of the transactions to which the rule will apply.[87] As the Blockchain Association notes, "The rule only addresses transactions between a hosted wallet and a self-hosted wallet controlled by a single counterparty, but that type of transactions accounts for a small and decreasing amount of total activity on public blockchains."[88] As a result, a large number of applications that use blockchain technology could fall under this rule's purview, which could harm their long-term development.[89]

As the Electronic Frontier Foundation describes, one such promising innovation is the development of "smart contracts"—a blockchain-based computer program that allows musicians to be paid directly without the use of any intermediary.[90] Under this arrangement, anonymous wallets work as

---

[82] *The Economist*, "America used to be behind on digital payments. Not any more."

[83] See Sections III and IV for a longer discussion.

[84] Sanger, "Russian Hackers Broke into Federal Agencies, U.S. Officials Suspect."

[85] CSIS, "Significant Cyber Incidents."

[86] EFF, "Comments to FinCEN," 8–10.

[87] Blockchain Association, "Comments on FinCEN Rulemaking," 6, 9.

[88] Blockchain Association, "Comments on FinCEN Rulemaking," 6, 9.

[89] Blockchain Association, "Comments on FinCEN Rulemaking," 6, 9; EFF, "Comments to FinCEN," 8–10.

[90] EFF, "Comments to FinCEN," 8–10.

intermediaries in a decentralized exchange between artists and listeners.[91] Due to the absence of any names and addresses associated with these intermediary wallets, smart contracts have no way to comply with the newly proposed rule.[92] Although businesses and entrepreneurs can eventually develop technology for maintaining compliance, it will be cumbersome and will likely disincentivize the future development of blockchain-based innovations.

Innovative companies can also use similar blockchain-based technology for a range of other innovations. For instance, businesses and consumers can use a distributed ledger system to create a decentralized user-to-user file sharing system without a central server.[93] These diverse applications of blockchain technology are significantly different in scope than the cryptocurrency exchanges involving the private wallets that FinCEN seeks to target.[94] By imposing CTR-like regulations on these transactions, FinCEN can impede such technological innovations.[95] If that becomes the case, many businesses relying on smart contracts and other blockchain-based technologies might ultimately move to alternative jurisdictions with friendlier rules. Such a development would significantly hamper America's lead in FinTech and other industries that will benefit from these technological breakthroughs.[96]

For the reasons stated above, FinCEN should be careful not to implement policies that will create an undue burden for businesses and jeopardize U.S. leadership in financial technology and innovation.

Respectfully submitted,

Ryan Nabil
John Berlau
COMPETITIVE ENTERPRISE INSTITUTE
1310 L Street NW, 7th Floor
Washington, DC 20005
(202) 331-1010

[91] EFF, "Comments to FinCEN," 8–10.

[92] EFF, "Comments to FinCEN," 8–10.

[93] Blockchain Association, "Comments on FinCEN Rulemaking," 9.

[94] Blockchain Association, "Comments on FinCEN Rulemaking," 9.

[95] Blockchain Association, "Comments on FinCEN Rulemaking," 9.

[96] EFF, "Comments to FinCEN," 8–10; Blockchain Association, "Comments on FinCEN Rulemaking," 9.

ryan.nabil@cei.org
john.berlau@cei.org