[EFF Letterhead]

January 4, 2020

VIA ELECTRONIC FILING

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

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

Comments to the Financial Crimes Enforcement Network (FinCEN) on Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets

I. Introduction

The Electronic Frontier Foundation (EFF) respectfully submits this letter to voice its concerns about FinCEN's proposal to implement certain recordkeeping and reporting requirements for cryptocurrency transactions.[1] The proposed rule would require money service businesses such as cryptocurrency exchanges to collect identity data not just about their own customers, but also about non-customers who transact with their customers using their own cryptocurrency wallets. The rule would require regulated businesses to keep records of cryptocurrency transactions over $3,000 USD and to report cryptocurrency transactions over $10,000 USD to the government.

EFF is concerned that the proposed regulation would (1) undermine the civil liberties of cryptocurrency users, (2) give the government access to troves of sensitive financial data beyond what is contemplated by the regulation, (4) violate the Fourth Amendment, (5) fail to comply with international privacy standards, and (6) present unintended consequences for certain blockchain technology—such as smart contracts and decentralized exchanges—that could chill innovation. Based on the substantial potential harms of this proposed regulation, EFF urges FinCEN not to implement this proposal.

EFF is also troubled that the proposal appears to be a transparent attempt to push a midnight regulation through before the end of the current presidential administration. The unusually short comment period over the winter holiday means that many experts and other members of the public will not have the opportunity to provide feedback on the potentially enormous consequences of this regulation. We urge FinCEN to significantly extend the

[1] Financial Crimes Enforcement Network, U.S. Treasury Department, *Notice of Proposed Rulemaking*, *Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets*, available at https://www.federalregister.gov/public-inspection/2020-28437/requirements-for-certain-transactions-involving-convertible-virtual-currency-or-digital-assets.

comment period to a minimum of 60 days as well as to offer additional time for comments after it makes any adjustments to the proposed regulation. We also urge FinCEN to meet directly with innovators, technology users, and civil liberties advocates prior to implementing any regulations.

II. About the Electronic Frontier Foundation

EFF is a nonprofit civil liberties law and technology organization. Founded in 1990, EFF champions individual privacy, free expression, and innovation. With more than 35,000 members worldwide, EFF uses public education campaigns, impact litigation, open source technology projects, policy analysis, and grassroots activism to ensure that civil liberties are protected in the digital age.

EFF has been at the forefront of identifying and advocating for civil liberties issues implicated by emerging technologies since its founding. For example, in the 1990s, EFF successfully challenged—in the courts and in policy discussions—broad export controls that attempted to limit the distribution of strong public key encryption, a technology that now underlies the security of the modern Internet and the financial transactions that take place across it. In *Bernstein v. United States*—in which EFF served as counsel to the plaintiff—the Ninth Circuit Court of Appeals ruled that computer code is speech protected by the First Amendment and that laws restricting its publication are unconstitutional. This foundational legal concept helped shape the thriving technological ecosystem in the United States today. EFF has also brought litigation challenging unconstitutional surveillance, including lawsuits challenging National Security Letters and certain warrantless mass surveillance programs of the National Security Agency. In addition, EFF's groundbreaking technology projects help to enhance security and protect privacy; for example, EFF's Certbot is a tool used by more than 20 million websites to encrypt content and protect their users' privacy and security, and EFF's Privacy Badger defends web browser users from being secretly tracked by advertisers and other third parties.

EFF allows its supporters to make donations through Bitcoin, Ethereum, Zcash, Litecoin, Dash, Dai, and other cryptocurrencies, including directly to EFF's wallets. EFF has provided testimony and public comments[2] on proposed cryptocurrency regulations in the past to voice the concerns of technology users, innovators, and civil liberties advocates.

Like the open Internet, cryptocurrency networks are a form of open source innovation that can enhance the freedom and privacy of technology users. EFF's mission to ensure that

[2] Electronic Frontier Foundation, *EFF, Internet Archive, and Reddit Oppose New York's BitLicense Proposal* (Oct. 21, 2014), available at https://www.eff.org/press/releases/eff-internet-archive-and-reddit-oppose-new-yorks-bitlicense-proposal; Rainey Reitman, *EFF and Open Rights Group Defend the Right to Publish Open Source Code to the UK Government*, Electronic Frontier Foundation (Aug. 16, 2019), available at https://www.eff.org/deeplinks/2019/06/eff-and-open-rights-group-defend-right-publish-open-source-software-uk-government; Rainey Reitman, *SEC's Action Against Decentralized Exchange Raises Constitutional Questions*, Electronic Frontier Foundation (Feb. 12, 2019), available at https://www.eff.org/deeplinks/2019/02/secs-action-against-decentralized-exchange-raises-constitutional-questions.

technology supports freedom, justice, and innovation is directly implicated by proposed regulations that would derail new cryptocurrency innovation, increase government surveillance, and hamper the civil liberties of technology users.

III. The Proposed Regulation Would Undermine the Civil Liberties of Cryptocurrency Users

Even in an increasingly digital world, people have a right to engage in private financial transactions. Cryptocurrency offers a way to bring to the online world some of the civil liberties benefits that people have long enjoyed when using cash. The proposed regulation would undermine these civil liberties benefits.

The ability to transact anonymously is instrumental to protecting Americans' civil liberties. Anonymity is important precisely because financial records can be deeply personal and revealing: they provide an intimate window into a person's life, revealing familial, political, professional, religious, and sexual associations—what organizations a person donates to, what family members a person supports, what services a person pays for, and what books and products a person buys. The ability to transact anonymously allows people to engage in First Amendment–protected political activities, including attending public protests and donating to advocacy organizations—activities that may be sensitive or controversial. As just one example, photos from the recent Hong Kong pro-democracy protests showed long lines at subway stations as protestors waited to purchase tickets with cash so that their electronic purchases would not place them at the scene of the protest. These photos underscore the importance of anonymous transactions for civil liberties. For the same reasons, dissidents in Belarus protesting to the reelection of the president[3] and protestors in Nigeria campaigning against police brutality[4] turned to cryptocurrency. Those anonymous transactions should be protected whether those transactions occur in the physical world with cash or online.

Cryptocurrency is also important for civil liberties because it is resistant to censorship. For years, EFF has documented[5] examples of traditional financial intermediaries shutting down accounts in order to censor otherwise legal speech. For example, financial intermediaries have cut off access to financial services for social networks,[6] independent booksellers,[7] and

[3] Anna Baydakova, *Belarus Nonprofit Helps Protestors With Bitcoin Grants*, CoinDesk (Sep. 9, 2020), available at https://www.coindesk.com/belarus-dissidents-bitcoin.
[4] Sandali Handagama, *Nigeria Protests Show Bitcoin Adoption Is Not Coming: It's Here*, CoinDesk (Oct. 21, 2020), available at https://www.coindesk.com/nigeria-bitcoin-adoption.
[5] Electronic Frontier Foundation, *Financial Censorship*, available at https://www.eff.org/issues/financial-censorship.
[6] Jeremy Malcolm, *Payment Processors Are Still Policing Your Sex Life, and the Latest Victim Is FetLife*, Electronic Frontier Foundation (Mar. 15, 2017), available at https://www.eff.org/deeplinks/2017/03/payment-processors-are-still-policing-your-sex-life.
[7] Rainey Reitman, *Legal Censorship: PayPal Makes a Habit of Deciding What Users Can Read*, Electronic Frontier Foundation (Aug. 21, 2018), available at https://www.eff.org/deeplinks/2012/02/legal-censorship-paypal-makes-habit-deciding-what-users-can-read.

whistleblower websites,[8] even when these websites are engaged in First Amendment–protected speech. In some of those cases of financial censorship, the censored organization has turned to cryptocurrency in order to continue to do business. For that reason, cryptocurrency transactions are generally more sensitive than other financial transactions. Cryptocurrencies have served as a vital lifeline for websites and online speakers who find themselves suddenly in the bad graces of a traditional payment intermediary, and who often have no other recourse. For those who seek to support these online speakers, cryptocurrencies may offer a privacy-protective, reliable alternative to financial channels governed by extra-legal policies of corporations.

The proposed regulation would require money service businesses such as cryptocurrency exchanges to collect identity data about non-customers who transact with their customers using their own cryptocurrency wallets. The proposed regulation would require these services to keep that data and to provide it to the government in some circumstances, such as when the dollar amount of transactions in a day exceeds a certain threshold. This would mean that people who store cryptocurrency in their own wallets would effectively be unable to transact anonymously with those who store their cryptocurrency with a custodial service.

FinCEN's language surrounding the use of "unhosted" wallets could be read to imply there is something unusual, or even nefarious, about wallets that are not "hosted," or that cryptocurrency is by default maintained by custodians. In reality, these independent stores of cryptocurrency are the fundamental provider of security and privacy for individual cryptocurrency users—just as people have long relied on cash for individual financial privacy and security.

IV. The Proposed Regulation Would Give the Government Access to Troves of Sensitive Data, Even Beyond What the Proposal Contemplates

The amount of sensitive data the government would be able to glean from its proposed new rule is vast, undercutting claims that the rule is narrow. The proposed regulation purports to require cryptocurrency transaction data to be provided to the government only when the amount of the transactions exceed a particular threshold. However, because of the nature of public blockchains, the regulation would actually result in the government gaining troves of data about cryptocurrency users far beyond what the regulation contemplates.

For some cryptocurrencies like Bitcoin, transaction data—including users' Bitcoin addresses—is permanently recorded on a public blockchain. For each Bitcoin transfer, the information that is publicly displayed includes the Bitcoin address of the sender and the receiver—an alphanumeric string akin to a username, which a user can use once or for multiple transactions. Bitcoin addresses are pseudonymous, not anonymous—and the Bitcoin blockchain is a publicly viewable ledger of all transactions between these addresses. That

[8] Esther Addley and Jason Deans, *WikiLeaks Suspends Publishing to Fight Financial Blockade*, The Guardian (May 31, 2017), available at https://www.theguardian.com/media/2011/oct/24/wikileaks-suspends-publishing.

means that if you know the name of the user associated with a particular Bitcoin address, you can glean information about *all* of their Bitcoin transactions that use that address.

The proposed regulation requires that money service businesses collect identifying information associated with wallet addresses and report that information to the government for transactions over a certain threshold. But when the government learns the identity associated with a particular cryptocurrency address, it will also know the identity associated with *all* transactions for that cryptocurrency address (which are publicly viewable on the blockchain), even when the amounts of those transactions are far below the reporting threshold. While the identity associated with the counterparties to those other transactions may not always be known, the government's database may well also contain that information because of the breadth of the proposed regulation. This means that the proposed regulation would actually provide the government with access to a massive amount of data beyond just what the regulation purports to cover.

The government may imagine that collecting additional information about cryptocurrency users is not problematic in and of itself, and thus this implication of the proposed regulation is acceptable, but this could not be farther from the truth.

A database can become a honeypot of information that tempts bad actors, or those who might misuse it beyond its original intended use. Thousands of FinCEN's own files were recently exposed to the public, making it clear that FinCEN's security protocols are not adequate to prevent even large-scale leakage.[9] This is not the first time that a sensitive government database has been leaked, mishandled, or otherwise breached. Over the past several weeks, the SolarWinds hack of U.S. government agencies has made headlines, and details are still emerging.[10] As just a few other examples, a hack of the Office of Personnel Management exposed over 22 million personnel records[11] and a breach of a voting records database led to the personal information of over 190 million Americans being published online.[12] It's clear that government databases can and frequently do suffer from data breaches—whether through intentional leaks, hacks by bad actors, or negligent security practices—and thus the government should avoid collecting and storing unnecessary data. This is especially true for data as sensitive as the physical locations and identities of individuals associated with their financial transactions.

---

[9] Noam Scheiber and Emily Flitter, *Banks Suspected Illegal Activity, but Processed Big Transactions Anyway*, New York Times (Sep. 20, 2020), available at https://www.nytimes.com/2020/09/20/business/fincen-banks-suspicious-activity-reports-buzzfeed.html.
[10] David E. Sanger et al., *Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit*, New York Times (Dec. 14, 2020), available at https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html.
[11] Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, Washington Post (July 9, 2015), available at https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.
[12] Jim Finkle and Dustin Volz, *Database of 191 Million U.S. Voters Exposed on Internet: Researcher*, Reuters (Dec. 28, 2015), available at https://uk.reuters.com/article/us-usa-voters-breach-idUKKBN0UB1E020151229.

V. The Proposed Regulation Violates the Fourth Amendment

The proposed regulation violates the Fourth Amendment's protections for individual privacy. Our society's understanding of individual privacy and the legal doctrines surrounding that privacy are evolving. While 1970s-era court opinions held that consumers lose their privacy rights in the data they entrust with third parties, modern courts have become skeptical of these pre-digital decisions and have begun to draw different boundaries around our expectations of privacy. Acknowledging that our world is increasingly digital and that surveillance has become cheaper and more ubiquitous, the Supreme Court has begun to chip away at the third-party doctrine—the idea that an individual does not have a right to privacy in data shared with a third party. Some Supreme Court Justices have written that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[13] In 1976, the Supreme Court pointed to the third-party doctrine in holding in *U.S. v. Miller*[14] that the then-existing Bank Secrecy Act reporting requirements did not violate the Fourth Amendment.

Two developments make continued reliance on the third-party doctrine suspect, including as the source for regulations such as those contemplated here.

First, since the *Miller* decision, the government has greatly expanded the Bank Secrecy Act's reach and its intrusiveness on individual financial privacy. Although the Supreme Court upheld the 1970s regulations in an as-applied challenge, Justice Powell, who authored *Miller*, was skeptical that more intrusive rules would pass constitutional muster. In *California Bankers Association v. Shultz*, Justice Powell wrote, "Financial transactions can reveal much about a person's activities, associations, and beliefs. At some point, governmental intrusion upon these areas would implicate legitimate expectations of privacy."[15] Government intrusion into financial privacy has dramatically increased since *Miller* and *Shultz*, likely intruding on society's legitimate expectations of privacy and more directly conflicting with the Fourth Amendment.

Second, since *Miller*, we have seen strong pro-privacy opinions issued from the U.S. Supreme Court in multiple cases involving digital technology that reject the government's misplaced reliance on the third-party doctrine. This includes: *U.S. v. Jones* (2012),[16] in which the Court found that law enforcement use of a GPS location device to continuously track a vehicle over time was a search under the Fourth Amendment; *Riley v. California* (2014),[17] in which the Court held that warrantless search and seizure of the data on a cell phone upon arrest was unconstitutional; and *Carpenter v. U.S.*,[18] in which the Court held that police must obtain a warrant before accessing cell site location information from a cell phone company. EFF

[13] *United States v. Jones*, 565 U.S. 400, 417 (Sotomayor, J. concurring).
[14] 425 U.S. 435 (1976).
[15] 416 U.S. 21, 78-79 (1974) (Powell, J. concurring).
[16] 565 U.S. 400 (2012).
[17] 573 U.S. 373 (2014).
[18] No. 16-402, 585 U.S. ___ (2018).

is heartened to see these steps by the courts to better recognize that Americans do not sacrifice their privacy rights when interacting in our modern society, which is increasingly intermediated by corporations holding sensitive data. We believe this understanding of privacy can and should extend to our financial data. We urge FinCEN to heed the more nuanced understanding of privacy rights seen in modern court opinions, rather than anchoring its privacy thinking in precedents from a more analog time in America's history.

VI. The Proposed Regulation Must Demonstrate Compliance With International Privacy and Data Protection Principles

The expanded reach of the proposed regulation may interact in novel ways with existing privacy and data protection law outside the United States. Obtaining the identity of the owner of a wallet can reveal the wallet owner's previous transaction records, allowing precise conclusions concerning the private lives and financial habits of the individuals concerned. While such disclosures' asserted purpose is to "verify the identity of the customer," it clearly involves or requires the disclosure or processing of a wider set of data: it cannot be treated as merely obtaining the wallet owner's identity.

As such, government access to such data may trigger legal safeguards under international and foreign laws, including independent judicial authorization, legal and factual elements demonstrating that the disclosure of information is relevant to the criminal investigation and particular transactions, the respect of the principles of necessity and proportionality, public transparency reporting and oversight mechanisms, mandatory notification to the targeted individual at the earliest opportunity to ensure access to remedies, and a fixed list of information that a request must contain so providers can challenge and reject disproportionate or unnecessary demands.

For guidance, critical safeguards rooted in international human rights law are identified in the Necessary and Proportionate Principles on the Application of Human Rights, its global and Inter-American Legal analysis, and Privacy International Guide to International law,[19] as well as in the recent case law of the European Court of Human Rights concerning the Protection of Personal Data.

The current proposal does not outline how this regulation would seek to resolve such potential conflicts of law between the United States and other jurisdictions. We urge FinCEN to consult with colleagues at the European Data Protection Board and comparable institutions internationally, and make clear how the proposals will respect the necessity and proportionality requirements of international law, and the data protection regulations of other countries. Without

[19] Necessary and Proportionate Coalition, *Global Legal Analysis* (May 2014), available at http://necessaryandproportionate.org/global-legal-analysis; Privacy International, *Guide to International Law and Surveillance 2.0* (Feb. 2019), available at https://privacyinternational.org/sites/default/files/2019-04/Guide%20to%20International%20Law%20and%20Surveillance%202.0.pdf; Katitza Rodriguez et al., *The InterAmerican Legal Analysis*, Derechos Digitales and Electronic Frontier Foundation, available at https://necessaryandproportionate.org/americas-legal-analysis.

such clarity, there is a risk that the enforcement of these broader regulations would lead to legal challenges in Europe and elsewhere and create legal uncertainty for the affected institutions.

VII. The Proposed Regulation Would Have Unintended Consequences for Blockchain Technology, Chilling Innovation

The proposed regulation would have unintended consequences for smart contracts and other decentralized technology with a wide range of lawful uses, and could chill blockchain innovation.

Under the proposed rules, money service businesses would have to collect certain identity information—such as names and physical addresses—about wallet users who transact with their customers. That requirement is problematic for several reasons: first, it presupposes that the wallets that their customers transact with are tied to particular humans; in reality, many such wallets will be part of an automated system with which the user transacts. Second, even when the counterparty to a transaction is a person, the proposed regulation would add friction to transactions, making it significantly more difficult for cryptocurrency users to interact with others who use a service subject to the regulation.

Despite the name, "wallets" are not just personal stores of currency tied to particular individuals: they are often a way for computing systems to hold and dispense money without relying on institutions. Blockchain technologies such as "smart contracts" enable the automatic execution of transactions between wallets without necessarily requiring the involvement of intermediaries or the involvement of humans at all. Wallets are not always caches of digital money held by users; rather, a wallet is often one link in a chain through which an automated, frictionless transaction is executed. Tokens stored in "wallets" may represent more than just money—they may, for example, be tied to permissions and unlocking requirements around personal data, or they may provide transparency into the automatic execution of an agreement when a condition is met.

"Smart contracts" can be conceptually simplified to "programmable money," and have a wide range of lawful use cases beyond basic financial transactions. Being able to send value directly to others with no intermediary enables programmers to write computer code that automatically transfers value when a condition is met. As one example, in the music industry, decentralized applications like Audius already use smart contracts to transfer money from users directly to musicians—automatically, and without any intermediary between the user and the musicians.[20]

We are in the very earliest days of the exploration of smart contract technology. Just as it would have been an error to see the early Internet as merely an extension of the existing postal service, it is important not to view the risks and opportunities of smart contracts strictly

[20] We offer Audius not to draw attention to this particular application, but as one example of the many types of innovation we can expect to see in this space in the future.

through the lens of financial services. Smart contract technology should not be broadly regulated by the Department of the Treasury; while FinCEN has a key role in this space, regulations should be carefully tailored—with input from the industry and experts—to avoid unintended consequences for a broad swath of emerging technologies. This proposed regulation in particular would have unintended consequences that could hinder smart contract development. The regulation's requirement that money service businesses collect identity information for wallets that are counterparties to their customers' transactions is impossible to comply with when the counterparty is not a person but rather part of a smart contract system.

This regulation could also have a serious impact on the development of decentralized exchanges, a new technology utilizing smart contracts that seeks to address consumer needs that are not being met by existing financial services. Many people obtain digital currencies through centralized cryptocurrency exchanges. Blockchains themselves are decentralized, and transactions on blockchains are resistant to censorship. However, centralized exchanges act as choke-points through which users must pass to begin participating in the network; thus, financial censorship is most easily conducted at centralized exchanges. We have already seen examples of centralized exchanges mishandling user funds and betraying the trust of customers. Centralized exchanges can freeze the funds of customers, block certain customers from the platform, or block specific transactions, with no obligations to provide affected customers with an appeals process. Centralized exchanges can suffer outages, hacks, or losses that prevent customers from accessing their digital currencies. These centralized exchanges are also a target for criminals seeking to steal customer funds, and can themselves be run by unscrupulous individuals who abuse their access to customer funds and data.

Decentralized exchanges, by contrast, allow for the peer-to-peer exchange of digital currencies using smart contracts. For example, requests to sell and purchase cryptocurrency can be submitted to a smart contract that matches and completes these exchange transactions. Decentralized exchanges generally do not need to hold funds for customers; rather, customers maintain possession of their cryptocurrency, and the decentralized exchange can automatically execute exchange transactions without taking possession of the assets. Decentralized exchanges thus generally do not possess a central honeypot of money that might attract criminals like centralized exchanges do, and cannot themselves steal funds. Because transactions on decentralized exchanges do not require an intermediary, they cannot be easily censored by a single entity. Decentralized exchanges are an area of rapid research and innovation, and many cryptographers and programmers are experimenting with other trustless smart contract applications that may have significant public benefit in the long term.

FinCEN should be extremely cautious about crafting regulation targeting "unhosted" wallets in order to avoid interfering with the growing ecosystem of smart contract technology, including decentralized exchanges. The proposed regulation would not only chill experimentation in a field that could have many potential benefits for consumers, but would also prevent American users and companies from participating when those systems are deployed in other jurisdictions.

VIII. The Process for This Rulemaking Is Unusual and Improper

In addition to EFF's concerns with the substance of this proposed regulation, EFF is deeply concerned with the unusual and improper process surrounding this rulemaking. The 15-day comment period is unusually short and coincides with the winter holiday. This abbreviated comment period will no doubt prevent many concerned experts and users from offering feedback on the proposed regulation's deficiencies. These regulations require at least the regular 60-day comment period, and also demand a far broader debate given the potential effects on civil liberties and innovation.

While the Notice of Proposed Rulemaking points to alleged "threats to United States national interests" to justify the abbreviated comment period, the NPRM does not explain what the threat is, how that threat might be exacerbated by a 60-day comment period, or how a 15-day comment period over the winter break might benefit national security. Rather, the abbreviated comment period appears to be a transparent attempt at imposing a midnight regulation before the end of this presidential administration. However this regulation is implemented, it will happen under the next administration. That administration should have the opportunity to engage with the public about this proposal and ultimately decide whether to implement it.

IX. Conclusion

EFF appreciates the opportunity to submit comments to FinCEN on its proposed regulations. Because of the proposed regulation's potential impact on the civil liberties interests of technology users and potential chilling effect on innovation across a broad range of technology sectors, we urge FinCEN not to implement this proposal as it stands. We also urge FinCEN to provide at least 60 days for comment in order to correct the serious abnormalities of this rulemaking process and to ensure that civil liberties experts, innovators, technology users, and other members of the public have an opportunity to voice their concerns about the potential impact of the proposal.

Respectfully submitted,

Marta Belcher
Special Counsel
Aaron Mackey
Staff Attorney
Danny O'Brien
Director of Strategy
Rainey Reitman
Chief Program Officer

Electronic Frontier Foundation
(415) 436-9333