Analyzing FinCEN's Proposed Regulation Relating to AML and KYC Laws

Aaron Wright[1](✉) and Sachin Meier[2]

[1] Cardozo Law, Yeshiva University, New York City, USA
aaron.wright@yu.edu
[2] Georgetown University, Washington DC, USA

Keywords: FinCEN · Anti-money laundering · Financial crimes · NPRM · Privacy · Bitcoin · Cryptocurrency

1 Introduction

Questions related to anti-money laundering (AML) have pervaded policy conversations around blockchain technology for years. At their core, blockchains enable the rapid exchange of value, whether Bitcoin or other blockchain-based tokens, without the need to provide additional identity related information. With blockchains, value flows across the internet nearly as seamlessly as email and the technology is accessible to anyone with an Internet connection. Users of blockchain technology can remain pseudonymous, raising vexing questions related to the manner in which existing AML and related know-your-customer (KYC) compliance regimes should apply to this emerging technological ecosystem.

AML/KYC-related concerns have been long anticipated by proponents of technology involving strong cryptography, such as blockchains. For example, as far back as 1988, early cypherpunk and researchers Timothy May noted in his "Crypto Anarchist Manifesto" that "[t]he State will of course try to slow or halt the spread of . . . technology [involving strong cryptography], citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration" [1].

As even acknowledged by May, however, "many of these concerns will be valid" [1]. Blockchains create opportunities for technologists to reimagine and improve existing financial systems and its underlying infrastructure. At the same time, they create risks for abuse and misuse.

As the value of digital assets has exploded over the past several years, governments around the globe have begun to increasingly grapple with the question as to how AML/KYC rules should apply to blockchain technology. One of the latest attempts at this question was put forward for public comment by the United States Financial Crimes Enforcement Network (FinCEN), on December 18, 2020, through a notice of proposed rulemaking (the Proposal) along with a short set of FAQs regarding proposed requirements for certain transactions

M. Bernhard et al. (Eds.): FC 2021 Workshops, LNCS 12676, pp. 54–62, 2021.
https://doi.org/10.1007/978-3-662-63958-0_5

involving convertible virtual currencies (CVC) or digital assets with legal tender status (LTDA).

As discussed below, under the Proposal, if adopted, banks and money service businesses (MSBs) would be required to submit reports, keep records, and verify the identity of customers participating in transactions above certain thresholds involving blockchain-based wallets[1] not hosted by a financial institution (often referred to as "unhosted wallets") or wallets hosted by a financial institution in certain jurisdictions identified by FinCEN.[2]

The purpose of this paper is to provide an overview of FinCEN's latest proposal, outline public comments to this proposal, as well as to highlight certain legal challenges that the Proposal may face if it is adopted in its current form.

2 Overview of FinCEN Proposal

FinCEN is no stranger to grappling with questions relating to digital assets and cryptocurrencies. Starting in 2019, FinCEN issued guidance consolidating regulations, rulings, and prior guidance about digital assets and MSBs under the Bank Secrecy Act. FinCEN has also released an advisory to assist financial institutions in identifying and reporting suspicious activity or criminal use of cryptocurrencies.

The latest proposed rulemaking states that it was created in response to perceived concerns related to criminal actors' use of–and the national security risks posed by–certain digital asset-related transactions, involving assets on public permissionless blockchains. FinCEN cited concern that digital assets were being used to "facilitate international terrorist financing, weapons proliferation, sanctions evasion, and transnational money laundering as well as to buy and sell controlled substances, stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms, and toxic chemicals," and engage in ransomware attacks. FinCEN also stated a secondary

[1] A "wallet" allows a user to store, send, and receive cryptocurrency.

[2] The Proposal was made pursuant to the Bank Secrecy Act (BSA) and the proposed reporting and recordkeeping rules are similar to the rules for transactions in currency and for bank wire transfers, respectively. Relying on the Administrative Procedure Act's exemption from the 60-day comment period, FinCEN originally provided 15 days for public comment, or until January 4, 2021. However, FinCEN noted that it will endeavor to consider any material comments received after the deadline as well. On January 15, FinCEN extended the comment period for an additional 15 days for comments on the proposed reporting requirements, and for 45 days for comments on the requirement to report counterparty information and the recordkeeping requirements. In so doing, FinCEN noted the volume of comments received, as well as the enactment of the Anti-Money Laundering Act of 2020 (Division F) of Public Law 116-283 (AML Act), which amended 31 USC § 5312(a)(3), the definition of "monetary instruments" in the BSA, on which FinCEN proposes to rely in determining that CVC/LTDA are monetary instruments.

goal for the Proposal to establish controls to protect US national security from various state-sponsored threats, including state-sponsored ransomware and cybersecurity attacks, sanctions evasion, and the financing of global terrorism.

The proposed reporting requirement applies to CVC and LTDA transactions between a bank or MSB and a counterparty where: (1) the transaction exceeds $10,000 in value and (2) the counterparty uses an unhosted or otherwise covered wallet. The Proposal defines "otherwise covered" wallets as those held at a financial institution that is not subject to the BSA and is located in a foreign jurisdiction identified by FinCEN as a jurisdiction of primary money laundering concern, including Burma, Iran, and North Korea.

Transactions between hosted wallets and transactions where the counterparty wallet is hosted by a foreign financial institution, except for a foreign financial institution in a jurisdiction listed on the Foreign Jurisdictions List, would be exempt from the requirements. FinCEN plans to issue a value transaction report form similar to, but distinct from, the existing currency transaction reporting (CTR) form that will require the reporting of information on the filer, transaction, hosted wallet customer, and each counterparty. Pursuant to the Proposal, banks and MSBs will have 15 days from the date on which a reportable transaction occurs to file a report with FinCEN. The Proposal also includes an aggregation requirement if the financial institution has knowledge that a transaction is one of multiple CVC/LTDA transactions involving a single person within a 24-h period that aggregate to value in or value out of greater than $10,000.

In its January notice extending the comment period, FinCEN reiterated that it is not modifying the regulatory definition of "monetary instruments" or otherwise altering existing BSA regulatory requirements applicable to "monetary instruments" in FinCEN's regulations, including the existing CTR requirement and the existing transportation of currency or monetary instruments reporting requirement.

2.1 Recordkeeping and Verification Requirement

If implemented, the Proposal would require banks and MSBs to keep records of a customer's CVC or LTDA transactions and counterparties, and verify the identity of their customers, if a counterparty uses an unhosted or otherwise covered wallet and the transaction is greater than $3,000. They would also be required to verify the identity of the person accessing the customer's account, which may be someone conducting a transaction on the customer's behalf.

Consistent with a bank's or MSB's AML/CFT program, a bank or MSB would need to establish risk-based procedures for verifying their hosted wallet customer's identity that are sufficient to enable the bank or MSB to form a reasonable belief that it knows the true identity of its customer. For example, financial institutions should check FinCEN for the registration of a counterparty that purports to be a regulated MSB and for foreign financial institutions, and "would need to apply reasonable, risk-based, documented procedures to confirm that the foreign financial institution is complying with registration or similar requirements that apply to financial institutions in the foreign jurisdiction."

In addition, banks and MSBs would be expected to incorporate policies tailored to their respective business models should a bank or MSB be unable to obtain the required information, such as by terminating its customer's account in appropriate circumstances. The proposed recordkeeping and verification requirements would not apply to transactions between hosted wallets (except for otherwise covered wallets). Such transactions are already covered under existing AML requirements.

Unlike other recordkeeping requirements, the recordkeeping requirement in the Proposal would require the electronic retention of information based on the fact that such recordkeeping is the practical way in which businesses engaged in CVC or LTDA transactions are likely to track their data and the most efficient form in which data can be provided to law enforcement and national security authorities. Furthermore, the information must be retrievable by the bank or MSB by reference to the name or account number of its customer, or the name of its customer's counterparty.

2.2 Additional Data Collection

Under the Proposal, FinCEN expects that banks and MSBs would be able to employ a single set of information collection and verification procedures to satisfy both the reporting and the recordkeeping requirements. The data to be collected would include the following:

- The name and address of the financial institution's customer
- The type of CVC or LTDA used in the transaction
- The amount of CVC or LTDA in the transaction
- The time of the transaction
- The transaction hash
- The assessed value of the transaction, in US dollars, based on the prevailing exchange rate at the time of the transaction
- Any payment instructions received from the financial institution's customer
- The name and physical address of each counterparty to the transaction of the financial institution's customer
- Other counterparty information the secretary of the US Department of the Treasury may prescribe as mandatory on the reporting form for transactions subject to reporting pursuant to Sect. 1010.316(b)
- Any other information that uniquely identifies the transaction, the accounts, and, to the extent reasonably available, the parties involved
- Any form relating to the transaction that is completed or signed by the financial institution's customer

Notably, the Proposal does not impact direct peer-to-peer (P2P) digital assets or other blockchain-based transactions; rather, it only imposes a reporting and recordkeeping burden on banks and MSBs. However, the requirement will indirectly affect all users of unhosted wallets that engage in any transactions with banks and MSBs, which will be required to gather information from such users in order to comply with the new rule.

FinCEN has said that these new reports will allow law enforcement agencies to protect national security by more quickly and accurately tracking money flows to identify and stop terrorist attacks, drug and human trafficking, and cybercrime. However, there are questions as to whether the rule as written will accomplish these goals when parties generally set up a new wallet even for transactions that are fully compliant with the law. This can make the records kept and reported essentially useless with regard to tracking patterns of money flows to identify and stop bad actors.

3 Analysis of Public Comments

During the comment period, FinCEN received a number of public comments in response to the Proposal, despite a truncated notice and comment period. Roughly 7,500 people and entities submitted comments, the most FinCEN has received on any proposed rulemaking. The comments constitute nearly 70% of all comments FinCEN has received on all rule-makings since 2008 combined. An overwhelming majority of the comments published by members of the blockchain technology industry and individuals strongly opposed to the proposed regulation. Comments poured in from companies, software developers, advocacy groups, and individuals around the globe.

3.1 Institutional Responses

Several well-established institutions provided lengthy comments opposing the Proposal. Organizations at the forefront of the blockchain technology sector, such as Square, River Financial, Coinbase, and Fidelity Digital Assets pushed back against the proposed rulemaking, often highlighting the burdens of increased regulation and accompanying data collection. They also questioned whether the regulation would achieve its stated objective, given a concern that the Proposal failed to account for the technical operation of a blockchain. As pointed out by several institutions and blockchain experts, public blockchain-based wallets are nothing more than an address, raising complex questions related to ownership and control.

In addition, several institutions, including River Financial and Square Crypto, argued that the heightened compliance requirements created a risk that well intentioned individuals off of regulated exchanges and brokerages and onto newer, more user friendly decentralized platforms, due to cost, privacy concerns, or simple ease of use.

The number of users of blockchain-based decentralized finance (DeFi) services, such as decentralized exchanges (DEXs) is expanding. And, the Proposal's additional compliance requirements existing and new users of blockchain technology to migrate over to these newer services. Additional compliance increases the cost of these services and degrades the user experience, creating a motivation for users to migrate to potentially harder to regulate decentralized platforms.

New DeFi protocols such as Uniswap and Sushiswap enable seamless peer-to-peer exchanges in as little as a few clicks. These platforms are permissionless and do not currently incorporate any AML/KYC-related compliance. Volumes on these platforms have grown considerably over the past six months and are beginning to rival centralized exchanges. If regulation creates impediments to the use of centralized exchanges, users could increasingly migrate to these alternative services.

Alternatively, Bitcoin and other digital assets are easy to self-custody, giving customers the power to abandon regulated platforms, if regulatory requirements grow too cumbersome. As a result, the Proposal if implemented, will do "very little to stop bad actors, who face only the minor inconvenience of moving funds to a 'rule-compliant' wallet before moving them again."

3.2 Blockchain Developers

Concern was not raised solely by established institutions. The technologists pioneering and driving the responsible development of blockchain technology raised passionate objections to the Proposal. For example, Matt Corallo, a contributor to Bitcoin Core[3] and an employee of Square Crypto, raised several points about technical difficulties in implementing this rule, due to the inner workings of blockchain tech. For example, the Proposal requires the collection of additional information, but blockchains "do not include built-in mechanisms for banks or other forms of money services businesses to easily retrieve information like names and physical addresses. Due to these limitations, "[t]he only practical way in which a regulated entity could retrieve the counterparty information" would be to "force users to input that information directly when making a transaction."

3.3 Individuals

Users and enthusiasts of blockchain technology submitted the bulk of the public comments, offering comments of varying length and focus. As with institutions and developers, an overwhelming majority of individual responses objected to the Proposal, due to the:

- Burden of compliance
- Data collection and security

[3] Bitcoin Core is the reference implementation for Bitcoin. It is the source code which contains the consensus parameters and rules that define the Bitcoin protocol. Nodes run Bitcoin Core software in order to participate in the Bitcoin network. Read more about Bitcoin Core here: https://river.com/learn/what-is-bitcoin-core/.

- Inefficacy of Regulation, and the
- Short comment period[4]

4 Potential Legal Challenges

As highlighted in several public comments, the Proposal may face significant legal challenge in the United States on substantive grounds. The Proposal arguably violates the Fourth Amendment and may fail to comply with international privacy standards by giving the US government access to sensitive financial data beyond what is contemplated by the regulation.

The proposed regulation requires that MSBs 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 blockchain-based wallet, it also gains the ability to learn the identity associated with all transactions for that address (which are publicly viewable on a given blockchain), even when the amounts of those transactions are far below the Proposal's contemplated 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 could deanonymize all transactions on a blockchain, encroaching financial privacy.

In addition, any data collected by FinCEN could become a honeypot of information that tempts bad actors, or those who might misuse it beyond its original intended use. Indeed, thousands of FinCEN's own files were recently exposed to the public, raising questions as to FinCEN's security protocols. If sensitive data relating to blockchain users was made available to ill intentioned actors, blockchain users could face cybersecurity hacks, thefts, or other intrusions on financial privacy.

4.1 Fourth Amendment Concerns

The proposed regulation arguably violates the Fourth Amendment's protections for individual privacy. Historically, courts in the US have held that consumers lose their privacy rights in the data they entrust with third parties under the "third party doctrine". However, courts increasingly have become skeptical of these pre-digital decisions, reflecting evolving societal norms around privacy expectations.

[4] Institutions and individuals also complained about FinCEN's unusually short and poorly timed comment period. Coinbase published an entire comment solely dedicated to this issue, and requested that FinCEN extend the comment period to the traditional 60-day timespan. FinCEN initially released the 72-page Proposal in late December, such that the comment period would take place across Christmas Eve, Christmas Day, New Year's Eve, and New Year's Day. This circumstance provided minimal time for companies to digest the Proposal and formulate a proper, comprehensive response to the many flaws of the Proposal.

For example, the Supreme Court has begun to narrow the US's approach to the third-party doctrine, going so far as to note 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" [4]. Indeed, in California Bankers Association v. Shultz, the Supreme Court noted that, "[f]inancial 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" [5].

Due to the public and traceable nature of public blockchain, the Proposal runs the risk of dramatically increasing the scope of the government's knowledge about US blockchain user's financial privacy, potentially raising Fourth Amendment concerns.

4.2 International Privacy Concerns

The expanded reach of the proposed regulation likely will create new tensions with existing privacy and data protection law outside the United States. As noted above, obtaining the identity of the owner of a wallet often provides sufficient information to identify the wallet owner's previous transactional records, enabling the holder of this information to glean a greater range of information about the private lives and financial habits of the individuals or entities concerned.

Due to the nature of a blockchain, the contemplated disclosures would enable the government to gain access to a wider set of financial data, more than the identity of a given wallet's owner. Government access to such broad ranging financial data may trigger legal safeguards under international and foreign laws, which may require independent judicial authorization or the only permit the collection of such information with judicial consent, additional notifications, or other requirements.

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. Without such clarity, there is a risk that the enforcement of these broader regulations would lead to legal challenges in Europe and elsewhere creating further legal uncertainty.

5 Conclusion

FinCEN's Proposal aims to limit criminal and other socially undesirable activity through additional disclosure and reporting, in an attempt to create more reliable and trustworthy marketplaces where both blockchain technologists and existing entities can participate. However, as reflected in public comments, these additional requirements create practical challenges, due to the nature of the technology and the increased cost of compliance–both for covered entities and users. The Proposal may also face legal scrutiny in the US, given the potential breath of data collection available, and may create tensions with privacy and other data collection laws of other jurisdictions, requiring either further harmonization or creating a patchwork approach for entities operating globally.

Even if these practical and legal challenges are somehow addressed, users may choose to rely on more decentralized and emerging DeFi alternatives, due to simple ease of use, creating even more challenging regulatory concerns that would require an alternative approach to regulation. At the end, there would be a hard-to-navigate patchwork of legal rules and regulations that would not be consistent across different blockchain-related projects, companies, and use cases.

References

1. May, T.: The Crypto Anarchist Manifesto. https://www.activism.net/cypherpunk/crypto-anarchy.html
2. Scheiber, N., Flitter, E.: Banks Suspected Illegal Activity, but Processed Big Transactions Anyway, New York Times (2020). Available at https://www.nytimes.com/2020/09/20/business/fincen-banks-suspicious-activity-reports-buzzfeed.html
3. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf (2008)
4. US v. Jones, 565 U.S. 400, 132 S. Ct. 945, 181 L. Ed. 2d 911 (2012)
5. California Bankers Assn. v. Shultz, 416 U.S. 21, 94 S. Ct. 1494, 39 L. Ed. 2d 812 (1974)