GOODWIN

Goodwin Procter LLP
100 Northern Avenue
Boston, MA 02210

goodwinlaw.com
+1 617 570 1000

January 4, 2021

Financial Crimes Enforcement Network
United States Department of Treasury

Via Federal E-rulemaking Portal
Docket Number FINCEN-2020-0020
RIN number 1506-AB47

RE: Comments on behalf of CoinFlip to Notice of Proposed Rulemaking: Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets

On behalf of GPD Holdings LLC, d/b/a CoinFlip, the world's leading Bitcoin ATM operator, we offer the following comments to the notice of proposed rulemaking ("NPRM") by the Financial Crimes Enforcement Network ("FinCEN" or the "agency") regarding requirements for certain transactions involving convertible virtual currency or digital assets under the Bank Secrecy Act ("BSA"). 85 Fed. Reg. 83,840 (Dec. 23, 2020).

The agency's self-imposed rush has resulted in a flawed proposal that will impose new and unnecessary burdens—in key respects, more burdensome than the regime for traditional money transfers. And there is no justification for singling out virtual currency transfers in this arbitrary way. To the contrary, the rushed implementation of this proposal will pose particularly heavy compliance burdens for the many small businesses in the virtual currency space. Transfers will be halted while these businesses attempt to take the necessary time to build compliance procedures—time that the agency's end-of-year, end-of-administration scramble has denied them. And the benefits of requiring *more than a million person-hours of additional work* will be minimal at best, given that—as the agency acknowledges—true bad actors will still be able to evade or mislead the verification and reporting regime.

FinCEN wrongly asserts that it can bypass notice and comment.

The NPRM was made public on December 18, 2020, and published in the Federal Register on December 23, 2020, and the public was allowed only until January 4, 2021 to comment. The agency asserts that it is entitled to write these regulations without following the rulemaking requirements of the Administrative Procedure Act ("APA"), including the requirement to allow meaningful public comment, on two theories: because this rulemaking concerns "foreign affairs" and because it has "good cause" to dispense with the APA's requirements. Both are incorrect. The APA applies with full force to this rulemaking, and the agency is required to permit both a meaningful period of public comment and at least 30 days' notice of any final rule.

First, this rulemaking does not implicate the "foreign affairs" exception to the APA. *See* 5 U.S.C. § 553(a)(1). As the agency recognizes, that exception applies only to "matters affecting relations with other governments to a *substantial extent*, such as where adherence to the APA's requirements would 'provoke definitely undesirable international consequences.'" 85 Fed. Reg. at 85,853 (quoting H.R. Rep. No. 79-1980, at 23 (1946)) (emphasis added). By contrast, these

regulations reach purely domestic transactions; "the international consequence" is hardly "obvious." *East Bay Sanctuary Covenant v. Trump*, 932 F.3d 742, 776 (9th Cir. 2018).

The agency suggests that it can bypass notice and comment because the proposed rule "advances foreign policy and national security interests of the United States," but the notice recites generalities that would justify exempting *any* BSA rulemaking from the APA. 85 Fed. Reg. at 83,853. That has never been FinCEN's practice for general BSA rulemaking (as opposed to, for example, designating a particular country for the Foreign Jurisdictions List). To the contrary, the agency has frequently used notice-and-comment procedures when issuing regulations under the BSA, even when those regulations plainly relate to international financing. *See, e.g.*, 85 Fed. Reg. 68,005-06 (Oct. 27, 2020) (proposed rule would lower the threshold for reporting requirements for fund transfers "that begin or end outside of the United States); 75 Fed. Reg. 8,844 (Feb. 26, 2010) (proposed rule "clarif[ies] which person will be required to file reports of foreign financial accounts and which accounts will be reported"). Given its prior practice, it is clear that the agency has seized on this exemption to escape the consequences of its own delay and justify rushing this eleventh-hour rulemaking over an extended holiday period in the waning days of a lame-duck administration.

Moreover, FinCEN has failed to explain how a typical period of public comment will lead to "undesirable international consequences." *East Bay Sanctuary Covenant*, 932 F.3d at 776. The notice suggests that "[u]nduly delaying the implementation of the proposed rule would hinder the efforts of the United States government to perform important national security and foreign affairs functions," 85 Fed. Reg. at 83,853, but beyond vague generalities it fails "to offer evidence of consequences that would result from compliance with the APA's procedural requirements," *East Bay Sanctuary Covenant*, 932 F.3d at 776. The agency's professed concern about delayed implementation is also undercut by its decision to offer a limited public-comment period, demonstrating that there is no "need for immediate implementation." 85 Fed. Reg. at 83,853.

Nor has the agency established "good cause" for dispensing with the ordinary requirements of notice and comment. *See* 5 U.S.C. § 553(b)(B). "Good cause" does not just mean that the government finds it convenient to move faster. The exception is not an "'escape clause[]' that may be arbitrarily utilized at the agency's whim." *Mack Trucks, Inc. v. EPA*, 682 F.3d 87, 93 (D.C. Cir. 2012). Rather, the exception applies only in the very rare case where allowing public comment—which ordinarily serves the public interest—is affirmatively harmful to the public interest. The agency has not shown that to be the case here. All it offers is speculation that bad actors who currently have their assets in regulated financial institutions will rush to withdraw their funds if given time before the rule become effective—*but will not have already done so after learning of the agency's NPRM*. This prediction is precisely the type of barebones assertion—a conjecture "that someone will take advantage of the situation if advance notice is given"—that courts have deemed insufficient. *Mobil Oil Corp. v. Dep't of Energy*, 728 F.2d 1477, 1492 (Temp. Emer. Ct. App. 1983). And even if the agency's prediction were correct, the mere possibility that funds currently outside the BSA's purview will remain outside the BSA's purview is a far cry from the "significant threat of serious damage to important public interests" that courts have required in the past. *Id.* Finally, as with its use of the foreign-affairs exception,

FinCEN's reliance on good cause cannot be squared with its decision to provide *some* period of public comment. The exception is intended for "a situation in which the interest of the public would be defeated by *any* requirement of advance notice." *Util. Solid Waste Activities Grp. v. EPA*, 236 F.3d 749, 755 (D.C. Cir. 2001) (emphasis added) (quoting U.S. Dep't of Justice, Attorney General's Manual on the Administrative Procedure Act 31 (1947)). Here, however, the agency has plainly decided that public commenting will not undermine the purpose of the rule.

Because neither of these exemptions applies, two consequences follow. ***First***, FinCEN is required to permit a meaningful opportunity for public comment, which it has not done. Twelve calendar days—including *only four business days* when the government itself was open—is not remotely sufficient. *Cf.* Exec. Order No. 13,965, 85 Fed. Reg. 81,337 (Dec. 11, 2020) (closing the federal government on December 24, 2020). The industry cannot be expected to marshal economic and other empirical evidence to rebut the agency's flawed analysis in four business days. *See Prometheus Radio Project v. FCC*, 652 F.3d 431, 450 (3d Cir. 2011) (noting that 90 days is the "usual" length for a commenting period); Exec. Order No. 13,563, 76 Fed. Reg. 3821 (Jan. 18, 2011) (advising that a comment period "should generally be at least 60 days"). While CoinFlip is submitting a comment that highlights some particularly glaring problems with the proposed rule, it has not had nearly enough time to gather all the evidence necessary to provide a full picture of the rule's negative effects.

Where, as here, there is no pressing deadline or looming emergency, courts have been unwilling to condone agency efforts to rush through a complex rule. *See North Carolina Growers' Ass'n*, 702 F.3d at 770 (rejecting a 10-day comment period that did not reflect "the important interests underlying" a rule affecting visas for agricultural workers); *Pangea Legal Services v. U.S. Dep't of Homeland Security*, No. 20-cv-07721-SI, 2020 WL 6802474, at *20 (N.D. Cal. Nov. 19, 2020) (finding 30 days "spanning the year-end holidays" too short for a rule proposing substantial changes to asylum eligibility), *appeal docketed*, Case No. 20-17490 (9th Cir. Dec. 28, 2020). This is not the rare kind of case in which the agency faces a legal deadline to act and therefore has to truncate the comment period. *See, e.g., Fla. Power & Light Co. v. United States*, 846 F.2d 756, 772 (D.C. Cir. 1988) (15-day comment period was appropriate given impending Congressional deadline).

Moreover, any sense of urgency the agency feels (lack of deadline notwithstanding) is of its own making, having had this issue on its agenda for well over a year, *see* 85 Fed. Reg. at 83,852 (detailing supposed informal engagement on this issue going back to May 2019). "[G]ood cause cannot arise as a result of an agency's own delay." *Nat. Res. Def. Council v. Nat'l Highway Traffic Safety Admin.*, 894 F.3d 95, 114 (2d Cir. 2018) (internal quotations omitted). Because the agency waited to promulgate the proposed rule, there is now not "enough time with enough information to comment," nor is there enough time "for the agency to consider and respond to those comments." *Prometheus Radio*, 652 F.3d at 450.

Second, the agency may not make its final rule effective less than 30 days after publication. *See* 5 U.S.C. § 553(d). While expressing a desire to implement the final rule as soon as "feasible," the agency certainly has not shown that the new regulations can feasibly be implemented in less than the standard 30 days by the many small businesses on which the

burden will fall. And, for the same reasons explained above, the agency has not established a need for "immediate implementation," particularly when balanced "against principles of fundamental fairness" requiring that parties "be afforded a reasonable amount of time to prepare" for the regulation. *Omnipoint Corp. v. FCC*, 78 F.3d 620, 630 (D.C. Cir. 1996).

The proposed rules would impose a compliance regime for digital currencies that is more burdensome than the regime for traditional currency transfers, without justification.

FinCEN proposes to expand information-gathering requirements about counterparties to virtual currency transactions in a manner that does not exist today for traditional currency transactions. While the recordkeeping and reporting requirements in the proposed rule are based on existing rules for traditional currency transfers, virtual currency businesses do not have the same infrastructure that traditional banks and the larger, more established money services businesses ("MSBs") can use to collect and verify the information specified in the proposed rule. Moreover, the proposed rule will place significant additional burden on dynamic and emerging virtual currency businesses, many of which are not large banks or businesses, stifling innovation and disproportionately impacting these small businesses.

Although existing regulations require financial institutions (a defined term in BSA regulations) to collect and record certain information about the sender and recipient of the transfer, the difference in infrastructure would make meeting the requirement more burdensome for virtual currency businesses than for traditional banks and money transmitters. For nonbank money transfers of $3,000 or more,[1] a nonbank that initiates the transfer for the sender must (i) collect and record certain information about the sender and the transmittal order; (ii) verify the identity of the sender; and (iii) collect and record information about the recipient, including the name and address and the destination bank account number of the recipient, and any identifiers of the recipient that are included in the transmittal order. If a nonbank is accepting the transfer from the sender's bank, and delivering funds to the recipient, (i) the nonbank would have already been required to verify the identity of the recipient if the recipient is a customer that has opened an account, and (ii) if the recipient is not an established customer, the recipient's name and address must be recorded, and if the recipient is a person, the identity of the recipient must be verified, by collecting name, address, government identification, and social security number. *See* 31 C.F.R. § 1010.410(e).

Existing regulations do not require a receiving nonbank to confirm the name and address of the sender, though the name and address of a person can be obtained from the sender and verified through any number of public databases and the internet. A bank account number can also be obtained from the sender (which obtains it from the recipient) and verified through communication channels, such as SWIFT, that exist between banks today.

[1] We note that another NPRM proposes to reduce the threshold to $250 for funds transfers and transmittals of funds that begin or end outside of the United States, for the purpose of the Recordkeeping Rule and Travel Rule provisions set forth in 31 CFR §1010.410(e) and (f). 85 Fed. Reg. 68005 (Oct. 27, 2020).

By contrast, the proposed rule would require verification of the identity of hosted wallet customers who engage in transactions with unhosted or otherwise covered wallet counterparties in the amount of $3,000 or more. With respect to reporting requirements, the proposed rule notes that financial institutions should report, "at a minimum," the name and physical address of each counterparty, which suggests that additional information should be gathered, though the proposed rule does not provide further detail about what additional information should be required from the counterparties. 85 Fed. Reg. at 83,849. This requirement is broader and more burdensome than the existing rules for traditional currency transfers described above. Moreover, while a financial institution may gather the name and physical address of each counterparty, the proposed rule will have the unintended consequence of placing responsibility for verifying that information squarely on the financial institution. The agency acknowledges in the NPRM that "persons engaged in illicit finance will likely attempt to use falsified credentials," which would be of no use to law enforcement, but the agency provides no guidance for how MSBs and banks should address the issue, other than noting vaguely that "banks and MSBs develop solutions to ferret out abuse" without acknowledging that the available solutions do not detect and prevent all such abuse. 85 Fed. Reg. at 83,845 n.32. While the proposed rule does not expressly require financial institutions to verify information about each counterparty to the transaction, it may well have that effect in practice: the requirements to form reasonable belief about the provenance and characteristics of the counterparties' wallets, as discussed below, and to develop solutions to address the risks arising from the submission of false information, likely will effectively require financial institutions to verify the information collected to ensure that they can fully comply with the proposed rule and provide useful information to law enforcement.

Moreover, the proposed rule assumes that financial institutions are able to determine whether a wallet is hosted or unhosted, and puts the onus on financial institutions to "have a reasonable basis to determine that a counterparty wallet is a hosted wallet at either a BSA-regulated financial institution or a foreign financial institution in a jurisdiction that is not on the Foreign Jurisdiction List" in order to avail itself of the exemption for transfers to hosted wallets at such exempt financial institutions. 85 Fed. Reg. at 83,849. That saps the exemption of much of its utility. The "reasonable basis" standard appears nowhere in proposed § 1010.316(d) itself, leaving unclear how it would apply. Cryptocurrency blockchains commonly have limited information regarding cryptocurrency transactions, frequently only a wallet address.

In addition, the NPRM notes that "MSBs … would need to apply reasonable, risk-based, documented procedures to confirm that the foreign financial institution is complying with the registration or similar requirements that apply to financial institutions in the foreign jurisdiction." 85 Fed. Reg. at 83,849. It is not reasonable for an MSB to be able to assess another institution's compliance with laws of a foreign jurisdiction, with which the MSB is unlikely to be familiar; it is certainly not realistic for an MSB to be responsible for verifying compliance with the laws of *every* foreign jurisdiction to which it may send an occasional transfer. In making this assessment, the MSB would have to largely rely on the declarations of the foreign financial institution, which may be unreliable. Without access to that financial institution's internal compliance system or knowledge of foreign laws, it would be difficult to confirm whether those

declarations are true. That exercise is thus a clear example of the way in which the proposed rule imposes onerous burdens for no real benefit.

In sum, the proposed rules impose a compliance framework for virtual currency transactions that is more onerous than existing regulations for traditional currency transactions. It is unlikely that any bank or MSB will be able to confirm whether a wallet is unhosted, or whether a financial institution in a foreign jurisdiction is complying with the requirements applicable to it in the foreign jurisdiction. The result will be a severe curtailment of virtual currency transactions by banks and MSBs, and significant execution delays for those virtual currency transactions that are able to be executed. In a traditional money transfer, the financial risk of waiting a few minutes or hours to complete a transfer is not nearly as great as it is in a virtual currency transfer, because the value of a digital currency can fluctuate rapidly. Transaction delays place the parties at significant legal and financial risk, and may result in significant safety-and-soundness concerns, particularly where banks and MSBs are themselves counterparties to transactions.

Lack of clarity about the scope of the proposed rule creates compliance challenges.

The intended scope of the proposed rule does not match the actual language of the proposed rule, and at a minimum the agency should clarify the scope of the rule. The explanation in the NPRM states that the rule would require financial institutions to "identify and verify *hosted wallet* customers who engage in transactions with unhosted or otherwise covered wallet counterparties when those customers conduct transactions having an equivalent of $3,000" (emphasis added). 85 Fed. Reg. at 85,844. However, as drafted, proposed 31 C.F.R. § 1010.410(g) is broader than that description. The proposed recordkeeping and identity-verification requirements would apply to each "withdrawal, exchange or other payment or transfer, by, through, or to [a bank or MSB] which involves a transaction in convertible virtual currency or a digital asset with legal tender status with a value of more than $3,000," except for transactions with a counterparty whose account is held at a Bank Secrecy Act regulated financial institution or foreign financial institution not located in a jurisdiction identified on the List of Foreign Jurisdictions. 85 Fed. Reg. at 85,860. The rules would apply, among other circumstances, if a customer *without a hosted wallet* purchases convertible virtual currency having a value of $3,000 for cash or other convertible virtual currency and instructs that the purchased convertible virtual currency be sent to an unhosted wallet.

In addition, the proposed rule would require a financial institution to verify the identity of its customer engaging in a transaction covered by the rule "before concluding" the transaction. 85 Fed. Reg. at 85,859. FinCEN should clarify that this requirement only applies once and that a financial institution would not need to re-verify the identity of an existing customer whose identity has already been verified. There is an existing carveout from the identity verification requirements in 31 C.F.R. § 1010.410 and 31 C.F.R. § 1020.420 for "established" customers who have an account at the financial institution and from whom the financial institution has obtained certain identifying information. A similar carveout would be appropriate here as there does not seem to be any purpose served by requiring a financial institution to re-verify the identity of an established customer.

These ambiguities impose heightened compliance burdens because of the highly accelerated rulemaking timeline the agency has unnecessarily imposed. The rules were published less than two weeks ago, and the agency shows every sign of rushing to finalize them and make them effective. This shortened period reduces the time available to financial institutions to determine whether they need to change their internal processes to remain in compliance. Given the accelerated time period, banks and MSBs will likely need to pause transactions involving unhosted wallets until they are able to develop the tools, processes, and procedures to implement the requirements. Halting transactions is likely to cause significant financial harm and may, counterproductively, drive users to unregulated and anonymous platforms.

The proposed rule does not accurately consider the compliance cost to financial institutions.

The agency acknowledges that compliance with the proposed rule will result in a significant burden for MSBs. For example, FinCEN estimates the recordkeeping burden alone for each MSB will require 2,928 extra hours of employee time, or the equivalent of nearly two new employees per company. 85 Fed. Reg. at 83,858. FinCEN estimates an additional 533 extra hours per MSB for complying with the reporting requirements. 85 Fed. Reg. at 83,858. These are FinCEN's estimates alone; the limited comment period simply does not allow for most MSBs to calculate the additional burden in a meaningful manner. These implementation issues are exacerbated for small entities, which are not exempted from the proposed rule.

Moreover, the agency fails to calculate the cost of (i) storing the additional data, or (ii) reviewing and producing it in response to legal process. MSBs frequently receive legal process from the government and civil parties; the proposed rule would materially increase this burden as well.

The proposed rule raises significant privacy and data-security concerns.

The proposed rule requires financial institutions to gather an immense amount of data about individuals and wallets that, once gathered, must be stored for years, leading to the inevitable risk of data breaches. Data breaches may result in the public disclosure of the owners of these wallets, including relating to large holders of Bitcoin or other more public figures. This creates safety issues relating to the risks of ransom and extortion, in addition to privacy issues.

In addition, with respect to virtual currency transactions on public blockchains, such as with Bitcoin and Ether, once the government obtains an unhosted wallet holder's information via the reporting mechanism described in the proposed rule, the government, without requiring even a subpoena, would be able to track a person's financial transactions from that wallet from its inception many years earlier through the present – allowing for real-time monitoring of transactions – and for the entire time person holds the hosted wallet, which could be years in the future. This is extraordinary visibility for the government to have into an individual's transaction history with no cause or basis, and is, in fact, much broader and more invasive than a search warrant, wiretap, or subpoena.

The industry has a number of concerns that, without adequate time to comment, it is unable to fully document.

The proposed rule raises a number of concerns that the industry does not have time to adequately study, due to the compressed notice period. These concerns include the following:

- The proposed rule, by attempting to restrict transactions in virtual currency, will lead to such activity – both legitimate and illicit – moving to foreign jurisdictions, and will undercut the perceived benefit of the proposed rule to U.S. law-enforcement agencies.
- Blockchain and digital currency companies are more than payment systems; these companies can play a role in insurance, finance, and supply chain management innovations. The propose rule will stifle innovation and job creation at a time the country can ill-afford the further loss of jobs and technology overseas.
- By effectively preventing transactions in virtual currency unless banks and MSBs can verify the names and addresses of users, the proposed rule discriminates against the underbanked, including individuals with no fixed address.

For the foregoing reasons, the agency should either withdraw its proposed rules for further study or, at a minimum, reopen public comment for at least 60 days to permit stakeholders to document their concerns with the agency's proposal. Under no circumstances should the agency continue its headlong rush to implement this proposal without following the APA's core requirement: meaningful public participation, followed by reasoned consideration of the comments the public presents. The current schedule will allow for neither.

Respectfully,

/s/ Samantha M. Kirby Co-chair, Banking & Consumer Financial Services	/s/ Grant P. Fondo Co-chair, Digital Currency & Blockchain Technology	/s/ William M. Jay Co-chair, Appellate Litigation