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

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

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

December 22, 2020

To whom it may concern:

Coin Center is an independent nonprofit research and advocacy center focused on the public policy issues facing cryptocurrency technologies such as Bitcoin. Our mission is to build a better understanding of these technologies and to promote a regulatory climate that preserves the freedom to innovate using open blockchain technologies. We do this by producing and publishing policy research from respected academics and experts, educating policymakers and the media about blockchain technology, and by engaging in advocacy for sound public policy.

This letter is our comment on the proposed rule to implement a new recordkeeping rule for convertible virtual currency (CVC) transactions over $3,000 and apply existing currency transaction report (CTR) requirements to CVC transactions over $10,000.[1] Part 1 will focus on the process deficiencies inherent in the current rulemaking and Part 2 will address issues with the substance of the proposed rule.

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

On the Process of this Rulemaking

Before we address the substance of the proposed rule we will first address the process by which it is being promulgated. Administrative rule making is by its nature an undemocratic and potentially unaccountable activity through which an unelected bureaucracy, exercising broad delegated powers, enacts law that is binding on individuals with few if any checks. The Administrative Procedure Act (APA) was adopted by Congress in 1946 to serve as "the bill of rights for the new regulatory state" and "establish[] the fundamental relationship between regulatory agencies and those whom they regulate."[2] Central to the APA's process is "notice and comment" rulemaking.[3] "The essential purpose of according § 553 notice and comment opportunities is to reintroduce public participation and fairness to affected parties after governmental authority has been delegated to unrepresentative agencies."[4] Robust notice and comment is therefore what underpins the legitimacy of an otherwise undemocratic and unaccountable process.[5]

Typically, regulatory agencies afford the public at least 30 days to comment on proposed rules, and this is the minimum time recommended by the Administrative Conference of the United States.[6] In practice, regulatory agencies provide about 49 days on average.[7] Executive Order 12,866, which is binding on FinCEN, instructs agencies to "provide the public with meaningful participation in the regulatory process," including a "meaningful opportunity to comment on any proposed regulation, which, in most cases should include a comment period of not less than 60 days."[8] In the present rulemaking, the Treasury Department is affording the public only a 15-day comment period that straddles the Christmas and New Year's holidays, and is doing so in the midst of a global pandemic.[9] This is shameful. Giving the public effectively only a few

---

[2] George P. Shepherd, "Fierce Compromise: the Administrative Procedure Act Emerges from New Deal Politics," 90 *Nw. U. L. Rev.* 1557 (1995-1996).
[3] Antonin Scalia, "Judicial Deference to Administrative Interpretations of Law," 3 *Duke L. J.* 1989, 511-521 (1989).
[4] *Batterton v. Marshall,* 648 F.2d 694, 703 (D.C. Cir. 1980).
[5] Nina A. Mendelson, "Rulemaking, Democracy, and Torrents of E-Mail," 79 *Geo. Wash. L. Rev*. 1343, 1348 - 50 (2011).
[6] "Rulemaking Comments," Administrative Conference of the United States, Recommendation No. 2011-2, June 16, 2011, https://www.acus.gov/recommendation/rulemaking-comments.
[7] "Public notice and comment rulemaking (United States" Organization of Economic Cooperation and Development, 2016, https://www.oecd.org/gov/regulatory-policy/USA-Public-Notice-and-Comment.pdf.
[8] Executive Order 12866, F.R. Vol. 58, No. 190, October 4, 1993, https://www.archives.gov/files/federal-register/executive-orders/pdf/12866.pdf. That the opportunity to comment must be "meaningful" has been echoed by the courts. *See: N. Carolina Growers' Ass'n, Inc. v. United Farm Workers*, 702 F.3d 755, 770 (4th Cir. 2012); *Rural Cellular Ass'n v. FCC*, 588 F.3d 1095, 1101 (D.C. Cir. 2009).
[9] Excluding weekends and federal holidays, the period consists of eight work days including Christmas Eve and New Year's Eve.

days to study a complex proposal and develop meaningful comment—especially at this particular moment in the calendar—runs counter to the spirit, if not the letter, of the APA and demonstrates an unseemly contempt for the public.

How does the Treasury Department justify its departure from normal procedure? First, it cites a categorical exemption under § 553(a)(1), which states that the rule making process outlined in the APA does not apply "to the extent that there is involved a … foreign affairs function of the United States."[10] Because the present rulemaking involves a foreign affairs function, it argues, the Treasury Department has no obligation to provide the public with notice or an opportunity to comment.[11] Second, the Treasury Department cites a specific exemption to the obligation to provide notice and opportunity to comment if an agency finds "good cause … that notice and public procedure thereon are impracticable, unnecessary, or contrary to the public interest."[12] Specifically it argues that in this instance providing additional comment is unnecessary and contrary to the public interest.[13] We will address these claims in turn.

Foreign Affairs Function Exception

Courts have found that the "foreign affairs function" exception to the notice and comment rulemaking requirement "cannot apply to functions merely because they have impact beyond the borders of the United States."[14] Instead, as both the Senate and House Reports on the APA make clear, it applies to "only those 'affairs' which so affect relations with other governments that, for example, public rulemaking provisions would clearly provoke definitely undesirable international consequences."[15]

In the present rulemaking, the Treasury Department does not identify any specific undesirable international consequence of a 30-day rather than a 15-day comment period. Nor does it identify any relations with other governments that are implicated. Instead, it merely asserts that "[t]he proposed rule advances foreign policy and national security interests of the United States."[16] To support this contention it cites that its authority rests on the Bank Secrecy Act

---

[10] "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," Financial Crimes Enforcement Network, 31 CFR Parts 1010, 1020, and 1022, RIN 1506-AB47, [*forthcoming in Federal Register*] https://public-inspection.federalregister.gov/2020-28437.pdf; 5 U.S.C. 553(a)(1), (b)(3)(B), (d)(3).
[11] *Ibid*.
[12] *Ibid*.
[13] *Ibid.*
[14] *Mast Indus., Inc. v. Regan*, 596 F. Supp. 1567, 1581 (Ct. Int'l Trade 1984).
[15] Senate Committee on the Judiciary, "Administrative Procedure Act: Legislative History," S. Doc. No. 248, 79th Cong., 2d Sess. 19 (1947), https://coast.noaa.gov/data/Documents/OceanLawSearch/Senate%20Document%20No.%2079-248.pdf.
[16] *Supra* note 1, at 39.

(BSA), which was enacted by Congress "to respond to threats associated with international financial transactions."[17] It also argues that by its nature, virtual currency activity "involves cross-border value transfer or cross-border operations" and cites the fact that "[o]nly approximately 17% of the nodes on the Bitcoin network operate in the United States."[18] By this standard, it is difficult to imagine how any rule proposed by FinCEN would not be subject to the "foreign affairs function" exception. After all, the BSA underlies almost all of FinCEN's authority, and any rulemaking that implicates the internet for money transmission would be exempt since the vast majority of nodes on the internet operate outside the U.S.[19]

Again, the fact that the proposed rule would have effects outside the U.S. is not sufficient to deny the public a meaningful opportunity to provide comment. The exception exists for situations in which providing notice and an opportunity for public comment would itself affect relations with foreign governments by provoking undesirable international consequences.[20] The Treasury Department does not argue that the present rulemaking is such a situation. Furthermore, the "foreign affairs function" exception is categorical; it relieves a qualifying rulemaking from all the requirements of § 553 presumably because engaging in them *at all* would create the negative international relations consequences that the exception seeks to avoid. In the current instance, by giving notice and inviting comment the Treasury Department is admitting that doing so does not have the kind of deleterious consequences the exception is meant to address. While the exception clearly allows for an agency to engage in *no* public rulemaking process, it is difficult to see how it can justify a crimped and rushed one. It does not make sense that a 15-day comment period does not "provoke definitely undesirable international consequences," but a 30-day comment period would.

Good Cause Exception

The other justification cited by the Treasury Department for limiting public comment is the "good cause" exception in § 553(b)(B).[21] That clause allows an agency to forgo Section 553's notice and comment requirement if "the agency for good cause finds" that compliance would be "impracticable, unnecessary, or contrary to the public interest."[22] The Treasury Department here does not claim that notice and comment is impracticable since, after all, it is seeking

---

[17] *Id*.
[18] *Id*. at 40.
[19] Richard Webb, "The greatest network the world has ever seen: The global internet map," *NewScientist*, October 23, 2019, https://www.newscientist.com/article/mg24432530-500-the-greatest-network-the-world-has-ever-seen-the-global-internet-map/.
[20] *Mast Indus., Inc. v. Regan*.
[21] 5 U.S.C. § 553(b)(B).
[22] *Id.*

comment, but it does argue that a comment period longer than 15 days is unnecessary and contrary to the public interest.

Treasury argues that the standard 30-day comment period is unnecessary because it "has directly engaged with the cryptocurrency industry on multiple occasions and in a variety of formats over the past year on the AML risks arising in connection with cryptocurrency and carefully considered information and feedback received from industry participants."[23] This is absurd for two reasons.

First, consultation with the *cryptocurrency industry* is not a substitute for consultation with the *public*, as the APA requires. Some of the instances that Treasury cites for the proposition that further consultation with the public is not necessary were limited, invite-only, off-the-record meetings. Yet there are fewer Americans employed in the cryptocurrency industry than there are Americans who are affected by this proposed rule because they are developers or users of the technology, whether individually, in business, or in the non-profit sector.[24] That industry's interests may have been taken into account by Treasury does not make taking comment from the rest of the public unnecessary.

Second, that an agency engaged in policy discussions with public interest advocates and members of industry before a rule is announced cannot be grounds for making notice and comment rulemaking "unnecessary" and thus subject to the "good cause" exception. Otherwise there would likely be no proposed regulation—from any agency—for which notice and comment could not be omitted. Conversations about policy between industry, non-profit advocates, and the government is a daily occurence, part and parcel of good governance, and could not possibly be a predicate for voiding notice and comment. If it could, it would be the exception swallowing the rule.[25] It would also create an incentive for public advocates never to engage

---

[23] *Supra* note 1, at 37.

[24] One study from Cambridge University estimated that there were roughly 2.9 million to 5.8 million unique active users of cryptocurrency in 2017. *See*: Garrick Hileman and Michel Rauchs, "Global Cryptocurrency Benchmarking Study," University of Cambridge Centre for Alternative Finance, April 2017, https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2017-04-20-global-cryptocurrency-benchmarking-study.pdf.

[25] "As an initial matter, federal courts appear to agree that the good cause exception is to be 'narrowly construed.' Executive agencies bear the burden of persuasion in convincing a court that good cause exists, and the exception is not to be used as an 'escape clause' to avoid rulemaking procedures when convenient for the agency. 'Bald assertions' by an agency that comments are unnecessary in a particular situation do not create good cause. Otherwise, the exception would swallow the rule. In other words, agencies must provide courts with a sufficient reason showing why good cause exists in order to justify bypassing Section 553's procedural requirements." *See*: Jared P. Cole, "The Good Cause Exception to

with the government for fear that their consultations would become a predicate to deny notice and comment rulemaking.

Furthermore, the engagements cited by Treasury (including a letter from Coin Center)[26] were about open policy questions in general, not about the specific proposed rulemaking now in question. Broad and general discussion about possible approaches to achieve public policy ends does not make unnecessary an opportunity to address a specific proposal.[27]

Treasury also argues that providing the public a standard 30-day comment period is contrary to the public interest because it could tip-off criminals who, given notice of the forthcoming rule, would move their funds before it came into effect. The proposed rule notice states:

> It has long been recognized that the APA's notice-and-comment requirements may run counter to the public interest "when the very announcement of a proposed rule itself can be expected to precipitate activity by affected parties that would harm the public welfare." This is especially so in connection with financial regulation where the "announcement of a proposed rule would enable the sort of financial manipulation the rule sought to prevent." In such circumstances "notice and comment could be dispensed with in order to prevent the amended rule from being evaded." As noted above, FinCEN is concerned about the consequences of undue delay in the implementation of the proposed rule, and in particular that such delay could accelerate or cause the movement of assets implicated in illicit finance from hosted wallets at financial institutions to unhosted or otherwise covered wallets, such as by moving CVC to exchanges that do not comply with AML/CFT requirements.[28]

Notice and Comment Rulemaking: Judicial Review of Agency Action," *Congressional Research Service*, January 29, 2016, https://fas.org/sgp/crs/misc/R44356.pdf.

[26] *Supra* note 1, at 38.

[27] "In addition to general notice of proposed regulations, and an opportunity for interested persons to communicate their views thereon to the relevant government officials, adequate public participation in the rule-making process also requires that the exact terms of a new rule be published a reasonable time before its effective date. Otherwise, even if the public has participated in the preliminary formulation of a rule, the final details of its text may not be known to interested parties until the date of its promulgation as law." *See*: Administrative Conference of the United States, "Recommendations and Reports of the Administrative Conference of the United States," U.S. GOI, 1974, page 232, https://www.google.com/books/edition/Recommendations_and_Reports_of_the_Admin/SY_QAAAAMAAJ?hl=en&gbpv=1&dq=%22In+addition+to+general+notice+of+proposed+regulations,+and+an+opportunity+for+interested+persons+to+communicate+their+views+thereon+to+the+relevant+government+officials%22&pg=PA232&printsec=frontcover

[28] *Id.* at 41, footnotes omitted.

This is a weak argument. Treasury correctly notes that the notice-and-comment process can run counter to the public interest "when the very announcement of the rule itself" can tip off criminals, and that in such cases notice and comment can be "dispensed with" in the public interest. In the present case, however, the Treasury Department has announced the rule. The legal predicate for invoking the public interest exception they cite is not operative. Treasury nevertheless goes on to attempt a sleight of hand, arguing that "undue delay in the implementation of the proposed rule" could cause criminals to move funds for illicit purposes.[29] But the public interest exception they cite applies when an agency forgoes notice altogether, not to justify a rushed and shortened comment period to avoid "undue delay."

By giving notice of the proposed rule, the Treasury Department is admitting that tipping-off criminals is not what it is really concerned about. (We will get to what the real concern is shortly.) Once a proposed rule has been announced there is nothing "undue" about affording the public a meaningful opportunity to comment. Treasury cannot expect us to believe that 15 more days of comment would produce an "undue" delay with consequences so serious that it justifies jettisoning the normal APA process. Additionally, Treasury does not cite any evidence to support the contention that 15 more days of public comment would create an "undue" delay that would undermine the rule's purpose; it cites only its own judgment and presuppositions. However, as the Congressional Research Service has noted in a comprehensive report of the "good cause" exception, "[C]onclusory claims by an agency of an emergency situation, unaccompanied by independent facts, are insufficient to constitute good cause."[30] Courts have refused to uphold a finding of good cause when agencies fail to provide evidence of potential harm beyond their own expertise and predictions.[31]

Other facts militate against a "good cause" justification for a short and rushed comment period. For example, according to Treasury the harm to be avoided in the public interest is an "undue delay in the implementation of the proposed rule," meaning a delay in the provision of cash transaction reports (CTRs) to FinCEN. However, this would be true only if FinCEN were in a position to technically ingest the flood of CTRs that will be forthcoming if and when this rule comes into effect. It is our understanding that this is not the case and it could take months. Historically, FinCEN has given regulated parties (and itself) 180 days to get their systems ready to handle a new required form.[32] Cutting the public comment period in half will make FinCEN no better off once the rule is final, especially if the 30-day period before a rule becomes

[29] *Id*. at 4, 38, and 41.
[30] *Supra* note 23, at 7.
[31] *Id*. at footnote 62, citing *Tennessee Gas Pipeline Co. v. F.E.R.C.*, 969 F.2d 1141, 1146 (D.C. Cir. 1992).
[32] 31 CFR § 1022.380(b)(3).

effective required by Section 553(d) is also waived as one would imagine would be the case if "undue delays" really hurt the public interest.

Additionally, this rule applies not only to cryptocurrencies, but to the newly formulated category of "legal tender digital assets" (LTDA). This is a category of assets that is being mentioned for the first time in this rulemaking and that aims to cover central bank digital currencies (CBDC). But save for the Bahamas, there is no other country that has officially adopted a CBDC and, to the best of our knowledge, no FinCEN-regulated financial institution supports such assets. It therefore makes no sense to speak of "undue delays" when it comes to such assets. Even if one were to accept that there can be no delay in implementing the rule with respect to cryptocurrencies, no such case can be made about LTDAs, so it is certainly not in the public interest to shorten the comment period with respect to them. If this were to be allowed, then agencies would be able to forgo comment on any rulemaking simply by combining it with another rule that would satisfy invoking a "good cause" exception.

What is Really At Issue

It should be obvious to anyone familiar with the history of administrative rulemaking that the current proceeding is an example of "midnight rulemaking."[33] At the end of an administration, officials often hurry to issue last-minute rules before they have to leave their positions.[34] They are motivated by what has been called the Cinderella Constraint: "as the clock runs out on the administration's term in office, would-be Cinderellas—including the President, Cabinet officers, and agency heads—work assiduously to promulgate regulations before they turn back into ordinary citizens at the stroke of midnight."[35] From all accounts, this is the behavior being presently exhibited by the Secretary of the Treasury.

If and when a court reviews this rulemaking to determine whether the Treasury Department's invocation of the "good cause" exception is valid, it won't escape the court's attention that this is an improper midnight rulemaking. It will be clear that providing the normal 30-day comment period would have put the consideration of the comments and the finalization of the rule in the hands of the next presidential administration. Discovery during a legal challenge will likely show that getting this rule finalized before January 20th was the primary motivation for rushing

[33] Jerry Brito and Veronique de Rugy, "Midnight Regulations and Regulatory Review," 1 *Admin. L. Rev*. 61, 163-196 (2014) http://www.administrativelawreview.org/wp-content/uploads/2014/04/Midnight-Regulations-and-Regulatory-Review.pdf.

[34] *Id*.

[35] Jay Cochran, III, "The Cinderella Constraint: Why Regulations Increase Significantly During Post-Elections Quarters," Mercatus Center at George Mason University, March 8, 2001, https://www.mercatus.org/system/files/The_Cinderella_Constraint%281%29.pdf.

it. Claims of "undue delays" or "undesirable international consequences" are just a pretext for subverting the normal APA process in order to finalize the rule before the end of this president's term, something that is decidedly not in the public interest.

As Judge S. Jay Plager of the Court of Appeals for the Federal Circuit has stated, "public virtue suffers from the rush to publish" during the midnight period between Election Day and Inauguration Day.[36] According to him, such a rush is "unseemly" and "the haste with which midnight regulations are pushed out the door results in a certain amount of sloppiness and makes control of the regulatory apparatus appear to be a Washington game."[37] Those involved in so rushing out this rule should be ashamed of themselves.

The current process is not just a subversion of the APA's guarantee of meaningful public participation, it is also an insult to, and a breach of trust with, the cryptocurrency ecosystem. The cryptocurrency ecosystem's work with the Treasury Department has to date been based on trust, not mere obligation. However, the process employed in the current rulemaking is a breach of that trust and conveys a serious lack of respect for the developers, entrepreneurs, lawyers, academics, and ordinary citizens that make up the ecosystem.

We attended meetings sponsored by the Secretary, and engaged in exchanges of information with FinCEN, in good faith and in the pursuit of shared goals. To see these engagements cited as reasons for denying us access to a standard APA process feels like a betrayal. The message sent is: don't engage with Treasury or it will be used against you. Banks do not seem to face similar treatment. For example, take the "Customer Due Diligence Requirements for Financial Institutions" rulemaking, which is aimed at similar high-risk transactions involving banks.[38] Not only did this rulemaking include 60 days for comment, but FinCEN took over five years to finalize it and bent over backwards to accommodate the banks.[39] Why should we be treated any differently? Not only are we treated differently, we are treated with contempt. This rulemaking

---

[36] William S. Morrow, Jr., "Midnight Regulations: Natural Order or Disorderly Governance," 3 *Admin. & Reg. L. News* 26, 3 (2001) https://www.americanbar.org/content/dam/aba/publications/administrative_regulatory_law_newsletters/adminlawspr2001.pdf.

[37] *Ibid*.

[38] "Customer Due Diligence Requirements for Financial Institutions," 31 CFR Part 1010, 1020, 1023, 1024, and 1026, RIN 1506-AB25, https://www.fincen.gov/sites/default/files/shared/CDD-NPRM-Final.pdf.

[39] "FinCEN started this rulemaking proceeding in 2012 but delayed it in response to significant criticism and controversy. To develop more support for the proposal, FinCEN held a series of public hearings on the issue and incorporated many suggestions to reduce the regulatory burden surrounding the definitions and application of the policy." *See*: Michael Volkov, "Customer Due Diligence and Beneficial Ownership," *Volkov Law Blog*, September 15, 2014, https://blog.volkovlaw.com/2014/09/customer-due-diligence-and-beneficial-ownership/

(and its truncated timeline) was announced just before 5 p.m. on the Friday before the week of Christmas, causing many of the persons with whom Treasury often works to have to cancel their family plans to attend to it. That's not how one treats a partner.

Finally, we should say that we draw a distinction between the staff and leadership at FinCEN and at the Treasury Department. From our engagements it is clear to us that FinCEN, as well as law enforcement and the intelligence community, are not pursuing a rushed process. Indeed, there is near consensus that there is no need for this rule at all. It is the political leadership at the Treasury Department that is insisting that this process be rushed to finalize the rule before the end of the presidential term and it alone is responsible for this subversion of the public interest.

On the Substance of the Proposed Rule

Given the time constraints imposed by this rulemaking's process, this comment is limited to addressing the proposed obligation to record specific information related to cryptocurrency transactions over $3,000.[40] In particular, we will discuss practical and constitutional deficiencies inherent in the proposed obligation to record the name and physical address of so-called counterparties to financial institution (FI) customers.[41]

Cryptocurrencies function like physical cash or negotiable instruments (*e.g.* checks or commercial paper), and, accordingly, it is logical that long-standing rules for financial institutions that apply to transactions in cash or checks would be proposed to also apply to transactions in cryptocurrencies.[42] While we strongly object to the process by which FinCEN is promulgating a new CTR requirement for cryptocurrency transactions,[43] we do not at this moment address the substance of that rule change because it essentially seeks parity with existing standards for cash.[44] It places cryptocurrency activities on a level playing field with legacy financial activities and it avoids the creation of technology specific rules that would treat functionally equivalent instruments differently because of policy-irrelevant technical details.

We cannot, however, accept the new recordkeeping requirement, and, for the reasons argued

[40] *Supra* note 1, at 31.
[41] *Ibid*.
[42] *See* e.g. Peter Van Valkenburgh, "The Need for a Federal Alternative to State Money Transmission Licensing," Coin Center, January 2018, https://www.coincenter.org/app/uploads/2020/05/federalalternativev1-1.pdf.
[43] *See* infra part 1.
[44] *Supra* note 1, at 16 (Section C(3)).

below, insist that it be reverted to the existing flexible standard that applies in the context of legacy payments.

A Quick Fix

As currently drafted the proposed rule creates the following reporting requirements for convertible virtual currency (CVC) payments in addition to existing requirements.

	Legacy Payments	**CVC Payments**
FI to FI (over $3,000)	Recordkeeping Rule,[45] Travel Rule[46]	Recordkeeping Rule,[47] Travel Rule[48]
FI to Individual (over $3,000)		Extraordinary Recordkeeping Rule **(proposed)**[49]
FI to Individual (over $10,000)	Currency Transaction Report,[50] Currency Recordkeeping Rules[51]	Currency Transaction Report **(proposed)**[52] **+** Extraordinary Recordkeeping Rule **(proposed)**[53]

To be clear, the proposed rule creates a double standard between legacy payments and CVC payments. Whereas payments from an FI to an individual are typically only subject to a CTR and general recordkeeping requirement for transactions over $10,000, in the CVC context these payments will also be subject to a special recordkeeping rule for transactions above $3,000 (which includes a mandatory requirement that customer counterparties be identified by name and physical address) *and* a CTR rule for transactions above $10,000.

The simplest solution to the problems inherent in the current proposal (discussed below) would be to eliminate the extraordinary recordkeeping requirement in the context of CVC transactions above $3,000. In the legacy payments context no such extraordinary recordkeeping rule exists for sub-$10,000 transactions from an FI to an individual. This is the

[45] For Banks at 31 CFR § 1020.410(a), and for non-bank FIs at 31 CFR § 1010.410(e).
[46] 31 CFR § 1010.410(f)
[47] For Banks at 31 CFR § 1020.410(a), and for non-bank FIs at 31 CFR § 1010.410(e).
[48] 31 CFR § 1010.410(f)
[49] *Supra* note 1, at 66.
[50] 31 CFR § 1010.311
[51] 31 CFR § 1010.410(a)-(c)
[52] 31 CFR § 1010.311
[53] *Supra* note 1, at 66.

case despite the fact that the majority of money laundering (both in absolute and relative terms)[54] occurs using legacy financial services rather than CVC. The proposed rulemaking offers no justification for the extraordinary rule in the case of CVC, and, as discussed, the truncated rulemaking process does not even allow for meaningful notice and comment that might enable the public to better understand the concerns motivating this special treatment. Moreover, in the absence of this special rule for CVC transactions, FIs will continue to collect and record much of the information sought. Regulated FIs already have a duty to develop a risk-calibrated anti-money laundering program, and recording the details of transactions greater than $3,000 would sensibly be a part of such programs, although this is a necessarily flexible requirement as discussed below.

If we cannot persuade FinCEN to abandon this extraordinary recordkeeping rule altogether, then we ask merely that the recordkeeping rule be made at least as flexible in the context of a CVC transaction from FI-to-individual as it is in the context of a legacy transaction from an FI to an FI. Here's how those standards currently diverge and how they can be brought into parity.

For CVC payments, the new rule proposes the below. Note particularly section (vii) which imposes an obligation to collect counterparty information irrespective of whether that information is provided to, or readily obtainable by, the FI, (emphases added):

(i) The name and address of the financial institution's customer;
(ii) The type of convertible virtual currency or legal tender digital assets used in the transaction;
(iii) The amount of convertible virtual currency or legal tender digital assets in the transaction;
(iv) The time of the transaction;
(v) The assessed value of the transaction, in dollars, based on the prevailing exchange rate at the time of the transaction;
(vi) Any payment instructions received from the financial institution's customer;
(vii) **The name and physical address of each counterparty to the transaction of the financial institution's customer, as well as other counterparty**

[54] While estimates are hard to come by for obvious reasons, current analyses suggest that money laundering in legacy currency far exceeds that in relatively novel cryptocurrencies. For example, the Financial Action Task Force (FATF) cites the United Nations Office on Drugs and Crime (UNODC) estimates that some $1.9 trillion was laundered in 2009, well before most cryptocurrencies existed. In contrast, the blockchain analytics firm Chainalysis estimated that some $2.8 billion in Bitcoin was laundered through exchanges in 2019. *See*: "How much money is laundered per year?" *FATF*, https://www.fatf-gafi.org/faq/moneylaundering/; "Money Laundering in Cryptocurrency: How Criminals Moved Billions in 2019," *Chainalysis Insights*, January 15, 2020, https://blog.chainalysis.com/reports/money-laundering-cryptocurrency-2019.

information the Secretary may prescribe as mandatory on the reporting form for transactions subject to reporting pursuant to § 1010.316(b);

(viii) Any other information that uniquely identifies the transaction, the accounts, and, to the extent reasonably available, the parties involved; and,

(ix) Any form relating to the transaction that is completed or signed by the financial institution's customer.[55]

For legacy payments, the recordkeeping rule (for both a transmitting FI[56] and a receiving FI[57]) requires several similar items but only requires transmitting FIs to record information about the payment recipient *as those items are received* and only requires receiving FIs to record information *if received from the sender*. Unlike the proposed CVC rule, this rule accommodates FIs that do not have complete information about all sides of the transaction. Emphases added:

(A) The name and address of the transmittor;
(B) The amount of the transmittal order;
(C) The execution date of the transmittal order;
(D) Any payment instructions received from the transmittor with the transmittal order;
(E) The identity of the recipient's financial institution;
(F) As many of the following items ***as are received*** with the transmittal order:
    (1) The name and address of the recipient;
    (2) The account number of the recipient; and
    (3) Any other specific identifier of the recipient; and
(G) Any form relating to the transmittal of funds that is completed or signed by the person placing the transmittal order.[58]

We believe that there is an easy fix for this lack of parity. FinCEN should simply revise the proposed rule to match the flexible accommodations afforded FIs in the context of legacy payments. It would look something like this (additions in bold):

(i) The name and address of the financial institution's customer;

(ii) The type of convertible virtual currency or legal tender digital assets used in the transaction;

[55] *Id*. at 66.
[56] 31 CFR § 1010.410(f)(1)
[57] 31 CFR § 1010.410(f)(2)
[58] 31 CFR § 1010.410.

(iii) The amount of convertible virtual currency or legal tender digital assets in the transaction;

(iv) The time of the transaction;

(v) The assessed value of the transaction, in dollars, based on the prevailing exchange rate at the time of the transaction;

(vi) As many of the following items as are received with the customer's transaction:

(A) Payment instructions received from the financial institution's customer;

(B) The name and physical address of each counterparty to the transaction of the financial institution's customer, as well as other counterparty information the Secretary may prescribe as mandatory **when available** on the reporting form for transactions subject to reporting pursuant to § 1010.316(b);

(C) Other information that uniquely identifies the transaction, the accounts, and, to the extent reasonably available, the parties involved; and,

(D) Any form relating to the transaction that is completed or signed by the financial institution's customer.

Alternatively, the proposed rule could simply omit the counterparty item (vii in the original). Item viii in the original ("Any other information that uniquely identifies the transaction, the accounts, and, to the extent reasonably available, the parties involved")[59] plainly creates a flexible yet clear obligation to collect information about all parties involved, including counterparties, if and when that information is "reasonably available."[60] Either omission of the counterparty item (vii) or the creation of an "as are received" caveat (as exists in the recordkeeping rule for legacy payments between FIs) would bring CVC recordkeeping rules into rough parity with rules for existing transactions, albeit applying them in both the FI to Fi context as well as the FI to individual context (in this sense the rule would still be somewhat stricter when CVC is the method of transaction).

An objection to doing this may be that in the legacy payments space, where these transactions are FI to FI, the unidentified counterparty will, ultimately, be identified by the other FI. In the CVC space when transactions are FI to individual, the ultimate counterparty may remain unidentified because they are self-custodying their CVC.

[59] *Supra* note 1.
[60] *Id*.

First, we remind FinCEN that there is no equivalent recordkeeping rule for legacy transactions between FIs and individuals,[61] so if there is any asymmetry in these rules, it is that the rules would be *stricter* in the case of CVC than in the case of legacy payments, not the reverse. Second, we'd argue that the application of a CTR requirement would continue to ameliorate any risk from unidentified parties for transactions over $10,000 just as it does in the legacy payments context. That is exactly why imposition of the CTR standard to CVC transactions is, at least, logical.[62] Altogether, our proposed modifications to the recordkeeping rule would reasonably cover the bases with respect to CVC AML policy for FIs: In cases where the transaction is taking place between FIs, the recordkeeping rule collects all the same information as in the legacy payments context. In cases where the transaction involves an FI and a non-FI, records are still kept thanks to the extraordinary recordkeeping rule for transactions above $3,000 albeit counterparty information is not always available, but the transaction is also treated like a currency transaction when above $10,000 and triggers an automatic report to FinCEN to account for risks potentially generated by the partially deficient records.

Making counterparty data recordation contingent on its availability would bring the proposed rule into rough parity with existing standards and avoid prejudicing new technologies. Failure to do so, as we describe in the remainder of this comment, will be prejudicial in the extreme, would place a significant drag on innovation, would impede law enforcement, and may, indeed, jeopardize the constitutionality of the surveillance regime.

As we shall now discuss, the proposed recordkeeping rule is prejudicial to new technologies.[63] It is, in effect, a "secret" and therefore undemocratic and extra-legal ban on certain types of

---

[61] There is a flexible requirement (31 CFR § 1010.410(a)-(c)) to keep records for certain transactional documents that customers' provide when they make or request a $10,000+ currency transaction, but it does not require specific items such as counterparty identification, and it, of course, does not apply at the sub $10,000 transaction level. For Banks but not for other FIs, there are flexible requirements to keep copies of checks and other information already provided to banks by customers for transactions greater than $100, but this requirement does not include any specific fields for counterparty identification or other records not typically obtainable by the bank (31 CFR § 1020.4100). There is a requirement to keep some specific records for transactions from FI to FI over $3,000 but this requirement makes collection of identity information for the recipient mandatory if and only if it is available to the FI (31 CFR § 1010.410(e)(1)-(f)(2)) and 31 CFR § 1020.410(a). Once again, there is *no* specific recordkeeping requirement to collect counterparty information for legacy payments from FIs to individuals.

[62] *Supra* note 1; *see also* Peter Van Valkenburgh, "A Midnight Rule for Cryptocurrency Transaction Reports," Coin Center, December 18, 2020, https://www.coincenter.org/a-midnight-rule-for-cryptocurrency-transaction-reports/.

[63] *Infra* "Prejudicial to New Technologies and Creates, in Effect, a Secret Ban on Otherwise Innocent Transactions" section.

otherwise innocent transactions.[64] It will hamper law enforcement efforts to track illicit payments activity by pushing more users of the technology to self-custody their own cryptocurrency.[65] Finally, it would mandate the unconstitutional, warrantless search and seizure of private information,[66] and would obligate financial institutions to keep and report to government lists of persons engaged in the exercise of their First Amendment rights to assemble anonymously.[67]

Prejudicial to New Technologies and Creates, in Effect, a Secret Ban on Otherwise Innocent Transactions

Unlike the proposed CTR requirement, the proposed recordkeeping rule change is not technology neutral. The new rule obligates financial institutions to collect specific types of information *if and only if* the transaction is being made with cryptocurrency.[68] The rule replaces, in the case of cryptocurrency transactions only, the existing flexible risk-based standards for data collection.[69] Therefore, this rule creates a double standard between legacy payments activities and cryptocurrency payments.

This divergent approach is not merely administrative or technical: it is a fundamentally different policy that will create compliance obligations so onerous for a significant slice of transaction types that these transactions will be, in effect, banned. This is not a cryptocurrency-specific rule to address a cryptocurrency-specific problem. The same identification "problem" exists with legacy payments but accommodations are made to enable FIs to maintain compliance even when some information about the transaction is unavailable. To explain, let's look at some hypothetical types of transactions implicated by the rule and the likely consequences.

---

[64] *Id*. examples 1-3.
[65] *Infra* "Hampers Law Enforcement by Pushing Cryptocurrency Users to Self-hosted Wallets" section.
[66] *Infra* "Mandates an Unconstitutional Warrantless Search and Seizure" section.
[67] *Infra* "Forces the Identification and Ongoing Surveillance of Persons Exercising Free Assembly Rights" section.
[68] Peter Van Valkenburgh, "A Midnight Rule for Cryptocurrency Transaction Reports," Coin Center, December 18, 2020, https://www.coincenter.org/a-midnight-rule-for-cryptocurrency-transaction-reports/.
[69] 31 CFR § 1010.410.

Example 1: Supporting Political Speech; Self-custodying **Sender.**[70]
A "KYC'd" customer of a regulated financial institution shares a Bitcoin payment address generated by her FI in order to receive tips from generous patrons who want to support her blogging that advocates for political change in a foriegn nation with a kleptocratic regime targeting ethnic and religious minorities. A patron who has also fled this regime wishes to make a substantial donation to promote her work. He leaves a comment on her blog saying he will donate and makes a Bitcoin transaction for $5,000 from a Bitcoin address that he secures himself using a hardware wallet. Indeed, the donor's familiarity with, and fondness for, hardware wallets stems from the role these tools played in protecting his family's fortune in the wake of political turmoil in his homeland. Similar fortunes held at corrupt state banks were unfairly confiscated by the ruling party and used to strengthen their hold on political power through a brutal campaign of organized violence and fear.

Nothing is illegal about this transaction, indeed it may even qualify as protected First Amendment expression.[71] This transaction is not even anonymous between its participants; the donor wants the recipient to know about his donation and comments to that effect on her blog. Nonetheless, when the blogger's financial institution is faced with an incoming Bitcoin transaction from the donor, all it sees is a $5,000 Bitcoin transaction message from an unknown Bitcoin address. As a policy, it alerts its customer of the incoming transaction and asks for the name and physical address of the counterparty for the incoming transaction. She does not, however, know this information. Indeed, she hadn't even yet noticed the comment on her blog from the donor. Putting two and two together, she realizes that the payment is probably the donation promised by the friendly reader of her blog. When she asks the donor in the comment section of her blog about the payment and for the requested identification information, she obtains no response. She suspects he does not want his address widely known because of fear of reprisal from the foriegn regime; she sympathizes as she often has similar fears. At this point, lacking the requisite counterparty information, the FI has few choices. It could simply refuse to credit her account, choosing instead the easier route of sending the money back to the

[70] The following is a fictional hypothetical. There are, however, several real world examples of dissidents utilizing cryptocurrency to fight oppressive regimes. *See, e.g.*: Yomi Kazeem, "How bitcoin powered the largest Nigerian protests in a generation," *Quartz Africa*, October 26, 2020, https://qz.com/africa/1922466/how-bitcoin-powered-nigerias-endsars-protests/; Anna Baydakova, "Belarus Nonprofit Helps Protestors With Bitcoin Grants," *CoinDesk*, September 9, 2020, https://www.coindesk.com/belarus-dissidents-bitcoin.
[71] *See, for example:* Ilya Shapiro, "The First Amendment Protects Both Political Donations and Campaign Spending," *Cato at Liberty*, May 14, 2013, https://www.cato.org/blog/first-amendment-protects-both-political-donations-campaign-spending.

otherwise unknown Bitcoin address,[72] or holding the money in a segregated account under the FI's name until identities become known. Either way, the blogger never gets the donation.

As these difficulties happen more frequently, the exchange eventually chooses to stop offering their customers Bitcoin payment addresses. Now our blogger is forced to use her email address, on record with the FI, as a way to solicit donations. Donors must sign up for an account with the FI in order to pay her at that address. The Bitcoin protocol does not support email addresses as payment addresses; the FI in this case simply keeps a private list of which email addresses match to which internal customer accounts. Users can pay bitcoin to the exchange and, if and only if they sign up with their email, name, and address, will the exchange credit that bitcoin to the account of the recipient. The rule has, in effect, reduced an open payments network to a glorified and overly complicated version of any legacy money transmitter. Payments must start and end at financial institutions; two numbers change on the institutions' centralized databases; these are Bitcoin payments in name only as nothing ever makes it to the blockchain and only customers of these institutions can participate. Our blogger is eventually forced to leave the financial institution because they continually freeze her donations. She suspects this is happening because the institution has been publicly announcing plans to begin offering services in the country about which she critically blogs. She leaves the FI in favor of custodying her own Bitcoin because so many of her donors are, given the nature of her cause, wary of surveilled payments and keeping money with potentially corrupt institutions.

Example 2: Supporting Those Left Behind; Self-hosted Recipient.[73]
An American citizen has fallen on hard times. She is an ex-convict and suffers from drug addiction. She has been homeless for the last three months as her already tenuous financial state worsened when she lost her job at a local bar that closed because of the pandemic. Unable to find work she tries to support herself by selling artwork made from salvaged metal. She finds several interested buyers and, for a time, she is optimistic. Modest recognition for her artistic talents bolsters her self-esteem that has been ravaged by the indifference and outright prejudice so often faced by former convicts and the homeless. The money transmitter that was, for a time, allowing her to accept payments in cryptocurrency as well as dollars freezes her

[72] Returning a payment from an unknown source could very well make the FI complicit in money laundering. Transactions from a self-custodied wallet will mix with every other transaction to the FIs pooled Bitcoin wallet and become indistinguishable from legitimate transactions.
[73] In offering this hypothetical we do not intend to make strong claims that cryptocurrencies are the best tools to address the plight of the homeless and disadvantaged in America. However, there are reports of homeless persons unable to obtain banking services turning to cryptocurrency payments as a free alternative. (*See, for example*: Daniella Hernandez, "Homeless, Unemployed, and Surviving on Bitcoins," *WIRED*, September 20, 2013, https://www.wired.com/2013/09/bitcoin-homeless/). The value of these systems is that they are yet another option in an increasingly cash-free and restrictive payments landscape. This rulemaking risks foreclosing that option.

account without providing justification. She calls their customer support line but the hold-times and automated responses paired with representatives who are unable to help make the situation seem hopeless. She decides to accept payments using a software wallet on her smartphone. This works for a time but upon the promulgation of this rule, even these payments become unreliable because she can't provide her buyers with a physical address. Accordingly, buyers who are trying to pay her using a hosted wallet find that their wallet provider refuses to send the bitcoin.

Her payments are typically not greater than $3,000, indeed she would be happy to sell her art for anything reasonable. Nonetheless, as an ex-con with poor credit and no permanent address she can't open accounts at hosted wallet providers or legacy financial institutions. She should be able to receive these small payments at her unhosted wallet address but finds customers are still unable to pay. What's happened is that exchanges, faced with large payments arriving from unidentifiable addresses, have chosen to drop support for all self-hosted Bitcoin payment addresses. When large payments come from these addresses and identification fails, the exchange is faced with the difficult decision of what to do with the funds. Should it send them back to the sending address? That could facilitate money laundering as the sender has effectively washed their coins through the large pooled wallet at the exchange. Should it claim them as abandoned property? Pay them to the state? Would this be challenged in the future in a lawsuit from a sender? Faced with these questions the exchange simply decides to only offer transactions to fully identified accounts even for small payments. Our unfortunate artist, already left behind by legacy financial institutions, finds that now she cannot even use new tools like Bitcoin.

Example 3: Supporting Innovation; Machine to Machine Payments.[74]
A group of Wi-Fi router manufacturers have developed an open CVC-based payment standard and computational Wi-Fi radios that can automatically connect to consumer smartphones and provide internet bandwidth at super-competitive rates while metering consumer payments for data by the kilobyte. Because of the flat interchange fees inherent in all legacy open payment methods like credit cards, these tiny payments are only economical when made using CVCs and

[74] This is a functional hypothetical; however, all of the technologies described are feasible (see our Lightning Network and micropayments backgrounders) and several start-ups have begun experimenting with metered Wifi and CVCs. *For an example, see*: Rob Pegoraro, "This startup wants to pay you—in cryptocurrency—to help build its network," *Fast Company*, November 15, 2019, https://www.fastcompany.com/90431578/this-startup-wants-to-pay-you-in-cryptocurrency-to-help-build-its-network. *For our backgrounders, see*: Elizabeth Stark, "Lightning Network," *Coin Center Backgrounder*, September 15, 2016, https://www.coincenter.org/education/key-concepts/lightning-network/; Chris Smith, "Micropayments," *Coin Center Backgrounder*, June 3, 2015, https://www.coincenter.org/education/key-concepts/micropayments/.

self-custodied layer-2 wallets, *e.g.* the Lightning Network.[75] The manufacturers are variously in negotiations with airports and train stations to install these radios so that users can automatically maintain good data connections while traveling. Rather than release a proprietary app where a user can make payments to the radios, the manufacturers make their radios payable from any CVC wallet to a self-hosted layer-2 wallet on the device itself.

Because payments are made directly to each device, installers and managers of the radios can accept payments from any consumer and can directly reap the benefits of those payments rather than rely on a fee-charging intermediary to monetize their provision of bandwidth. This arrangement also saves would-be bandwidth consumers from lock-in with any particular Wi-Fi provider. Consumers can use any CVC wallet on their phones to automatically pay any nearby radio, no matter who manufactured it or who installed and administers it, so long as it conforms to the open standards. A non-profit even develops an open source app that automatically scans the area for available bandwidth from these standardized radios and negotiates for the lowest price per kilobyte to the consumer. This automatic competitive shopping service is also made possible because of the open nature of the CVC payment system. Anyone—including charitable consumer-watchdog organizations not associated with the companies that manufacture the devices—can develop compatible machine-to-machine payment applications that empower the consumer rather than the provider of paid services.

This decentralized Wi-Fi service is successful. However, sometimes when installers of the radios sweep their received Wi-Fi payments from the individual wallets of their radios to a hosted wallet the transactions fail because they are greater than $3,000 and the FI cannot readily identify the counterparty. The various installers of the devices must make an extraordinary effort to inform their hosted wallet providers that these transactions are, in fact, coming from their own devices and not some stranger whose physical address they cannot provide. Worse, several would-be consumers of the devices' Wi-Fi, who wish to pay devices from their hosted wallet accounts, find their transactions blocked. These transactions are tiny but some FIs have begun blocking all transactions, big or small, to self-custodied wallets because it is a significantly easier policy to implement than a screening and identification policy for transactions over $3,000.

Despite this and other friction generated by the counterparty rule, the service is a success for both data providers and consumers. It consistently offers significantly more affordable bandwidth to consumers without creating monopoly effects from service provider lock-in; individual radio owners must compete to provide the cheapest data within any geographic region but can still earn a healthy return by contributing to this decentralized infrastructure,

[75] *Ibid*., Stark.

especially in regions currently underserved by cellular or wired service providers. Because the system only works consistently when users custody their own cryptocurrency on their own device, several persons who would otherwise keep their CVC with an FI choose to hold their own CVC. The rate of truly peer-to-peer payments using CVC blockchains skyrockets and blockchain analysis firms struggle to identify any personal information with respect to these purely peer-to-peer transactions that do not touch regulated FIs.

***

Hopefully these examples humanize the issues that will arise from the proposed rule. A black-letter standard offers financial institutions no flexibility in dealing with situations that would otherwise warrant a sensitive approach that recognizes equity, innovation, mercy, or common sense in implementing compliance obligations. Moreover, for large payments (as well as small payments if institutions choose to treat them similarly as a convenient collateral consequence), the rule would take a vibrant open payment system that services the politically marginalized and the economically disadvantaged without discrimination and turn it into a closed system that will inevitably leave the most needy behind. Even legacy financial institutions are able to deal in open payments. Cash, checks, and other negotiable instruments are open payments, and while they may trigger CTRs (a part of this rulemaking with which we do not take issue here), they are not effectively banned in circumstances where a particular counterparty cannot be identified. These institutions are allowed to make sensible determinations about these higher risk payments,[76] and that, meager though it is, is an essential safety valve for those persons otherwise left behind by the financial system for all the wrong reasons.

A legacy financial institution, such as a bank, would be unable to comply with the proposed recordkeeping rule in an analogous payments context that does not deal with cryptocurrencies. When a bank customer writes a check to a non-bank customer, for example, can the bank reliably identify the physical address of the counterparty? Plainly no. The check will include the recipient's name or business but it will not necessarily include their address. When a bank customer receives a check from a non-bank customer and has that check endorsed over to her name or made out to "cash," can the bank reliably identify the physical address of the check endorser? Plainly no, the endorsements are merely a chain of signatures written on the back of the check itself. These hypotheticals are directly analogous to circumstances where a cryptocurrency exchange's customer pays an "unhosted" wallet address or receives a payment from an "unhosted" wallet address.

[76] 31 CFR § 1010.410.

If the proposed rule was fairly and equally applied to identical circumstances involving checks, it would be impossible for regulated financial institutions to reliably comply. As with this rule, the bank might simply ask the customer to provide a name and physical address for their counterparty in every incoming or outgoing check payment, but the customer would often not have this information. She would then either need to fabricate an answer or else she would be unable to fulfill her bank's request, and her bank would need to forbid her from using checks as a mode of payment in that circumstance or else be out of compliance with the clear standard in the rule. This is, of course, not the state of affairs with respect to checks and recordkeeping requirements. Instead, a bank is simply obligated to collect information about counterparties and other items "as [they] are received" with the transmittal order.[77] The bank would, by rule, collect that information if it was available; it might seek additional alternative information from the customer if it was not available; it might—in extraordinary cases—file a suspicious activity report or refuse to honor a check altogether given a lack of identifying information and their risk-calibrated standards. Several potential approaches are available to the bank in this context based on reasonable judgements of relative risk and available information, but no specific counterparty recordkeeping approach, especially not a specific counterparty standard that is impossible to reliably satisfy, is required.

Therefore, FinCEN would not, we would argue, apply this recordkeeping requirement in the context of checks because it would, functionally, outlaw the usage of checks in most circumstances. If FinCEN wanted to outlaw the usage of checks, we would argue, then it should do so transparently and honestly by simply promulgating a rule outlawing their usage rather than feigning their continued legality while simultaneously imposing impossible obligations on regulated parties dealing in checks. We can only have meaningful public comment and democratic accountability for drastic policy choices that would outlaw widely used methods of payments if the proposed rules transparently and honestly assert the result they intend. If there is a desire to ban these activities then let's discuss that; do not attempt to do so sub-silentio in a veiled and rushed administrative procedure that few in the public will even understand.

[77] 31 CFR § 1010.410(e)(1)(F).

Hampers Law Enforcement by Pushing Cryptocurrency Users to Self-Custodied Wallets

As long as there are thinking people in the world there will exist the products of the human mind: numbers, words, and the stories, contracts, and software that they can build. A banking regulation might outlaw checks but it cannot stop people from passing debt obligations from one to another with written instruments. A central bank might choose to recall and destroy a state's entire supply of paper money, but it cannot stop people from treating metals or other durable items as currency in face-to-face transactions. Similarly, this rule may make it impossible for financial institutions to send or receive cryptocurrency from self-custodied addresses, but it cannot stop people from generating their own addresses and freely using them to send and receive cryptocurrencies. Addresses are simply the numerical products of certain mathematical operations, and the process of creating new addresses is simply the performance of math on a personal computer or smartphone; banning that process is nothing short of insisting that all citizens recognize that 2+2=5.[78]

This rule is not a ban on address generation. It is, instead, a *de facto* ban on many transactions between addresses generated by regulated exchanges and addresses generated by individuals. As such, this rule will likely make self-custodying cryptographic credentials significantly more appealing to innocent and criminal users of the technology alike. The likely consequence will be to accelerate the adoption of so-called "unhosted" wallets.[79] To offer one example, our organization, Coin Center, a Delaware-incorporated non-profit corporation[80] with 501(c)(4) tax status[81] will, for the reasons specified below, cease using hosted wallet providers exclusively for our fundraising activities and begin accepting donations at cryptographic addresses that we, ourselves, generate and host. Here is the address we have generated for the Bitcoin network:

bc1q490kgfn596tynyu2p5cwzsjx2j4fmr6g6g8lu6uc8qc8jh9568msuw3r2g

---

[78] Tuna Tore, "How to generate a Bitcoin address — Technical address generation explanation," *Hackernoon*, January 15, 2020, https://hackernoon.com/how-to-generate-bitcoin-addresses-technical-address-generation-explanation-rus3z9e.

[79] The term is something of a misnomer, as there is really no such thing as an"unhosted" wallet. There are merely wallets. Some wallets are operated by FIs and some by individuals, just as there is cash in a bank's vault and cash under an individual's mattress. We do not call the latter an "unhosted" mattress or speak of "unhosted" dollars.

[80] Information on our filings with the state of Delaware may be accessed by typing "Coin Center" into the state's online search portal: https://icis.corp.delaware.gov/ecorp/entitysearch/NameSearch.aspx.

[81] A copy of our determination letter establishing non-profit status by the IRS may be downloaded from: https://apps.irs.gov/pub/epostcard/dl/FinalLetter_47-1315917_COINCENTERINC_06102015_03.tif.

Coin Center's mission is to defend the rights of persons to build and use free and open cryptocurrency networks.[82] We assume this responsibility because these networks are unowned public goods. These networks are available for free to the public and there is no way to exclude persons who do not support their operation from reaping the benefits of their functionality. These networks are also non-rivalrous: every additional payment address on the network adds to, rather than detracts from, the value of the network itself. As a non-excludable, non-rivalrous service, cryptocurrency networks fit the paradigmatic example of a public good.[83] Public goods are chronically underproduced by the market because their benefits are not entirely captured by the persons suffering the cost of their provision.[84] Coin Center performs a modest but important maintenance function for these networks: we represent these technologies and the interests of their users to the government in the hope that they can remain free and open tools unfettered by unnecessary or ill-informed regulation. Coin Center, as a self-appointed defender of these public goods is also, itself, a public good. We, therefore, commit to organization as a non-profit and rely on donations to finance our operations.[85]

Our community of donors is passionate about the continued vitality and freedom of these networks. They, on the whole, believe that people should be held accountable for their actions and prosecuted if they are criminal. However, they also strongly believe that every person is innocent until proven guilty, and that any law that blocks or prevents innocent people from transacting, or predicates that transaction on some rigorous and privacy-invading surveillance regime, is an unreasonable prior restraint on free expression and economic liberty.

Previous to this rule, donors would be able to send us payments from hosted wallets or self-custodied wallets to our hosted wallet addresses at regulated financial institutions.[86] If this rule is implemented, our hosted wallet providers will likely be unable to process any incoming donations from self-hosted wallets over $3,000 (unless the transactions are somehow accompanied with the requisite name and physical address required by the rule). Some supporters may find ways to comply but others may object, preferring to remain anonymous, or, at least, preferring to identify themselves to us but not an inherently unnecessary third party (if we offer a self-custodied wallet address as an alternative). We will, therefore, be

---

[82] "About," Coin Center, https://www.coincenter.org/about/.

[83] *See, on open source software as a public good generally*: Scott Christley, Jin Xu, Yongqin Gao, and Greg Madey, "Public Goods Theory of the Open Source Development Community Using Agent-Base Simulation," University of Notre Dame, January 2004, https://www3.nd.edu/~oss/Papers/oss_public_goods.pdf.

[84] Paul Samuelson, "The Pure Theory of Public Expenditure," 36 *Review of Economics and Statistics* 4, pgs. 387-389 (1954) https://www.jstor.org/stable/1925895.

[85] *Supra* notes 80 and 81.

[86] For example, we have previously solicited donations with an address managed by Coinbase, a regulated custodian.

substantially hampered in our fundraising efforts if we continue to conduct them utilizing only hosted wallet providers who are subject to these newly-proposed recordkeeping and surveillance obligations. We can easily maintain our access to our donor community by abandoning exclusive use of centralized wallet services and custodying our own wallet at the following addresses that we have generated on computers within our offices. Again, here is the address for the Bitcoin network:

bc1q490kgfn596tynyu2p5cwzsjx2j4fmr6g6g8lu6uc8qc8jh9568msuw3r2g

We recount this internal policy shift to illustrate an important point.[87] Coin Center is not a criminal enterprise; we are an education and research-focused non profit organization.[88] Nonetheless, for self-evident reasons this rule will push us as well as countless other innocent parties to abandon custodial wallet providers in favor or self-custodied wallets. This will impose costs on our organization: we will lose the safety and consumer-protections inherent in trusted, well-established and regulated institutions as custodians for our funds.[89] But, more importantly to the aims of regulators, this will impose significant costs on law enforcement. Law enforcement benefits from a healthy coexistence of wallets maintained by regulated entities and wallets maintained by individuals.[90] Law enforcement benefits from persons making transactions between regulated and unregulated addresses because it gains useful insights into the movement of money when it combines publicly available information from the blockchain with private information held by regulated parties.[91] As more transactions move to purely peer-to-peer channels, law enforcement will lose the ability to rely on intermediaries as aggregators of information concerning the flow of illicit funds.[92] This proposal will substantially shift the cost-benefit calculus of ordinary users towards holding their own cryptocurrency. Rather than enhancing law enforcement visibility into these networks the proposed rule will blind authorities to the details of their operation.

---

[87] And also to clearly show our standing in potential future challenges to the rule as an aggrieved party and as a membership organization whose donors are entitled to constitutional protections under the 4th and 1st Amendments.

[88] *Supra* notes 80, 81, and 82.

[89] Peter Van Valkenburgh, "The Need for a Federal Alternative to State Money Transmission Licensing," Coin Center, January 2018, https://www.coincenter.org/the-need-for-a-federal-alternative-to-state-money-transmission-licensing/.

[90] Jason Weinstein, "How can law enforcement leverage the blockchain in investigations?" Coin Center Backgrounder, May 12, 2015, https://www.coincenter.org/education/policy-and-regulation/how-can-law-enforcement-leverage-the-blockchain-in-investigations/.

[91] *Id.*

[92] *Id.*

Mandates an Unconstitutional Warrantless Search and Seizure

As a warrantless data collection, retention, and reporting requirement, the proposed rule's constitutionality can be attacked under Fourth Amendment jurisprudence establishing that individuals retain a reasonable expectation of privacy over information that they do not voluntarily provide to third parties for a legitimate business purpose.[93] By mandating the specific collection of information about persons who are not even customers of a financial institution, the rule substantially oversteps the established constitutional bounds of acceptable warrantless searches and seizures by financial institutions.[94]

The Supreme Court has found that warrantless data collection on the part of financial institutions is constitutional in the narrow case where the information has already been voluntarily provided by the FI's customer and is retained for a reasonable business purpose by the FI.[95] This is the case with the existing recordkeeping rule which asks only for items of information "as [they] are received with the transmittal order."[96] The Court has not yet been asked to rule on the constitutionality of mandated warrantless data collection by FIs for (a) information that is not already provided by their customer, (b) information that is personal to someone with whom the bank is not in privity, or (c) information that is not essential or even relevant to the bank's conduct of particular payments activities. As we shall explain, there are strong arguments supported by recent Supreme Court precedent in adjacent circumstances[97] for why this sort of warrantless data collection would be unconstitutional.

For clarity, let's first review why the information sought in the new recordkeeping requirement is extraordinary for the purposes of Fourth Amendment warrant requirements. The information is not provided by the bank customer, the information is personal to someone with whom the bank is not in privity, and the information is not essential or even relevant to the bank's conduct of payment activities.

Customers voluntarily provide FIs with a host of personal information in order to obtain financial services. For obvious billing, technical support, and legal purposes an FI customer expects to need to provide various personal information to the FI such as their home address,

---

[93] U. S. Const. amend. IV, *see also*: Peter Van Valkenburgh, "Electronic Cash, Decentralized Exchange, and the Constitution," Coin Center, March 2019, https://www.coincenter.org/app/uploads/2020/05/e-cash-dex-constitution.pdf.

[94] We are speaking specifically of the obligation to identify and keep records about customer counterparties. *Supra* note 1, at 31.

[95] *California Bankers Assn. v. Shultz*, 416 U.S. 21 (1974) https://supreme.justia.com/cases/federal/us/416/21/.

[96] 31 CFR § 1010.410.

[97] *Infra* note 108.

phone number, and other means of contact. FI customers, therefore, reasonably expect that this information will be available at the FI and retained as FI records that may be the target of an investigation. As the Supreme Court has repeatedly held, once the customer voluntarily provides this information to an FI she loses her reasonable expectation that this information will remain private.[98] Accordingly, a warrant is not required to obtain this information.[99] The same is true of the checks she cashes, the signatures she provides, and the payment orders she passes to the FI.[100] While it has never been tested in court, the same would be rationally true of any equivalent CVC-related information (*e.g.* Bitcoin addresses, bid or ask prices, smart contract instructions, etc.) that a customer provides to an exchange or wallet provider in order to obtain exchange or custodial services.

As the Court has found, bank customers can "assert neither ownership nor possession"[101] of these customer identity and activity records; they are "business records of the banks."[102] The particular nature of these records as identifiers and instructions and the necessity of their revelation in order to conduct the instructed business with the identified parties is core to the customers' privacy expectations. The Court found that the "contents of the original checks and deposit slips" are not private correspondence, but rather they are "negotiable instruments to be used in commercial transactions."[103] In other words, no customer could reasonably expect this information to remain confidential because the information's semi-public revelation is, itself, essential to the conduct of banking.

The Court reached a similar conclusion in *Smith*.[104] In that case, customers lost their expectation of privacy with respect to the phone numbers they provided to phone companies while dialing to make a connection.[105] No customer could expect privacy in these numbers because every customer understands that the numbers must be revealed in order for the service provider to make a connection. As with the phone numbers dialed in *Smith*, bank customers understand that they must hand information over to the third party as a means to conducting business, else how would a bank know whom they wish to pay? As the Court found, "all the documents obtained contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[106] *That*, to be clear, is the standard for

---

[98] *California Bankers Assn. v. Shultz*; *United States v. Miller*, 425 U.S. 435 (1976) https://supreme.justia.com/cases/federal/us/425/435/.
[99] *Id.* and *Katz v. United States*, 389 U.S. 347 (1967) https://supreme.justia.com/cases/federal/us/389/347/.
[100] *Id*.
[101] *Id*., 440.
[102] *Ibid*.
[103] *Id*., 442.
[104] *Smith v. Maryland*, 442 U.S. 735 (1979) https://supreme.justia.com/cases/federal/us/442/735/.
[105] *Ibid*.
[106] *Id*., 435.

warrantless collection of bank customer information: was the information voluntarily conveyed to the bank and exposed to their employees in the ordinary course of business? Information that is not voluntarily conveyed and not exposed in the ordinary course of business may, in fact, still require a warrant to be searched and seized. It goes without saying that the Bank Secrecy Act's recordkeeping and reporting requirements operate without warrants and, therefore, utilizing its provisions to demand the recording or reporting of certain types of information may be unconstitutional.

The counterparty information demanded by this rule is a horse of a different color. This is information that is personal to the counterparty herself, not to the bank customer. It is the counterparty's privacy expectations that are at stake in a Fourth Amendment context, not the expectations of the bank customer. What are the counterparty's expectations? For one, the counterparty will—in almost every typical scenario—have no idea that they are in any relationship with a regulated financial institution whatsoever. The counterparty simply knows that they would like to be paid using the Bitcoin network and that, to do so, they must share a Bitcoin address with the person who is paying them. Note, specifically, that the counterparty shares this address with the FI's customer, person to person, *and not with the FI itself*. The FI's customer will then inform her FI that *this* is the address she wishes to pay.

Unless, the FI's customer informs the counterparty that she is paying using a hosted wallet rather than with a self-custodied wallet, the counterparty has no way of even knowing that she is about to receive a payment from an address controlled by a regulated financial institution. She will not know that a regulated financial institution is involved in the transaction and therefore will certainly not expect that her privacy rights may be compromised by virtue of merely receiving a Bitcoin payment. She does not voluntarily convey her physical address or name to anyone, and therefore she retains a reasonable expectation of privacy with respect to that personal information.

In *Carpenter*,[107] the Court went so far as to say that private information that is inadvertently communicated by persons to a third party may still remain within the person's reasonable expectation of privacy.[108] In that case, cellular subscribers provided detailed location information to cellular providers every time their phone pinged a cell-tower. Despite the voluntary nature of choosing to use cell phones or choosing to use some specific cellular provider, the court found that subscribers were not voluntarily providing this location data.[109] Therefore the court found that a warrant would still be required for law enforcement to obtain

[107] *Carpenter v. United States*, 585 U.S. __ (2018) https://supreme.justia.com/cases/federal/us/585/16-402/.
[108] *Ibid*.
[109] *Ibid*.

this data from cellular service providers.[110] A Bitcoin user voluntarily chooses to use the Bitcoin network, and may voluntarily share her Bitcoin address with someone who wishes to pay her, but this user certainly does not voluntarily share any other personal information (*i.e.* her legal name or physical address) merely because she is accepting a payment on that network. If that information was inadvertently communicated to a regulated FI, and if that FI was made to report that information in a CTR, SAR, or because of a warrantless subpoena, then the holding in *Carpenter* strongly suggests that this search and seizure would be unconstitutional.

This information is, indeed, very private. Merely linking a name to a physical address can compromise the privacy of the resident. Linking a Bitcoin payment address (which may indicate great personal wealth)[111] to a name and physical address is extremely destructive of the owner's privacy and indeed may jeopardize her safety as she may become a target of a kidnapping or extortion plot.[112] Additionally, there is a high likelihood that several of these records will be reported to FinCEN in SARs and CTRs and through subpoenas. FinCEN records have recently been the subject of extensive leaks[113] and a recent government-wide hack may have compromised even more data.[114] If FinCEN was to maintain extensive records of Bitcoin addresses and their associated legal owners and physical addresses, then it would be a substantially attractive target for hacking and the privacy and safety of persons in those records would be in profound jeopardy.

Returning to the expectation of privacy analysis, however, it is sufficient to show that the counterparty has no idea that by mere virtue of sharing her Bitcoin address she is forfeiting her right to privacy over the details of her name and physical address. Her privacy expectations have not changed one iota by virtue of receiving this payment and therefore any information linking her name and physical address to her Bitcoin address, if it were to somehow be obtained by a regulated financial institution (as the rule requires), should remain subject to a warrant

---

[110] *Ibid*.

[111] For example, one can observe the holdings of Bitcoin addresses by examining the block chain. In this early ledger entry, we can see that this address, believed to be controlled by the creator of Bitcoin Satoshi Nakamoto, contains 50 BTC, which is worth over $1 million today: https://www.blockchain.com/btc/block/000000006a625f06636b8bb6ac7b960a8d03705d1ace08b1a19da3fdcc99ddbd.

[112] Andres Guadamuz, "A Kidnap, a Ransom, and the Limits of Bitcoin as a Criminal Currency," *BREAKERMAG*, January 17, 2019, https://breakermag.com/a-kidnap-a-ransom-and-the-limits-of-bitcoin-as-a-criminal-currency/.

[113] Jason Leopold, et al., "The Fincen Files," *Buzzfeed News*, September 20, 2020, https://www.buzzfeednews.com/article/jasonleopold/fincen-files-financial-scandal-criminal-networks.

[114] Kevin Collier, "Treasury also hacked in suspected Russian campaign, Mnuchin says," *NBC News*, December 21, 2020, https://www.nbcnews.com/tech/security/treasury-also-hacked-suspected-russian-campaign-mnuchin-says-n1251938.

requirement before it can be searched and seized by the state. Indeed, merely deputizing exchanges to obtain this personal information on behalf of the state and without a warrant is, by consequence, a government order to perform an unconstitutional seizure of personal information.

Controlling authorities[115] require that the information be both voluntarily provided (we have shown that it would often not be in the case of counterparty information) as well as exposed and retained for "legitimate business purposes."[116] Does a financial institution have a legitimate business purpose for collecting and retaining counterparty information? Coin Center does not represent any institutions subject to this rule, but directs FinCEN to their comments which will, we expect, explain in detail why obtaining this information would be, far from "legitimate," downright difficult and counter to their "business purposes."[117] From a technical point of view there is absolutely no need for this information to be collected. The Bitcoin protocol requires only a validly formed payment address, the amount to be sent, and the source of the bitcoins to be sent (*i.e.* a previous transaction on the blockchain) in order for a transaction to be valid and added to the blockchain.[118] As a provider of access to the Bitcoin network, there is no more a legitimate purpose for FIs to collect counterparty information than there is for a car manufacturer to collect facial recognition data from the vehicle's safety cameras, or for a genetic testing provider to collect tax returns alongside saliva swabs.

The technology behind a cryptocurrency transaction is designed to obviate the need for users to hand any personal data over to any third party.[119] Indeed, these systems are designed such that no trusted third party need even exist for the transaction to take place.[120] A user will construct her electronic messages to be compatible with the cryptocurrency protocol that she chooses to use. This data alone may be useful to regulators and law enforcement,[121] but it will certainly not include typical financial transaction data like the name or physical address of the user. Irrespective of its usefulness to law enforcement, this is the only data that a user of these

---

[115] *California Bankers Assn. v. Shultz*, *United States v. Miller, Carpenter v. United States*.
[116] *United States v. Miller, Carpenter v. United States*.
[117] See, for example, this summary comment from the Kraken exchange: "FinCEN's New Rule Is About to Wall Off the Poor from Our Financial System Forever," Kraken FX Blog, December 21, 2020, https://blog.kraken.com/post/7286/fincens-new-rule-is-about-to-wall-off-the-poor-from-our-financial-system-forever/.
[118] Eric Wall, "How Private is Bitcoin?" *Human Rights Foundation*, March 7, 2019, https://medium.com/human-rights-foundation-hrf/privacy-and-cryptocurrency-part-i-how-private-is-bitcoin-e3a4071f8fff.
[119] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008, https://bitcoin.org/bitcoin.pdf.
[120] *Id*.
[121] Paige Peterson, "Anatomy of A Zcash Transaction," *Electric Coin Company blog* (Nov. 23, 2016) https://z.cash/blog/anatomy-of-zcash/.

protocols must provide in order to obtain the desired result and, consequently, it is the only data for which a user directly interacting with the protocol would no longer have a reasonable expectation of privacy.

Users of hosted wallets lose this reasonable expectation of privacy with respect to a greater range of data because, unlike a person who custodies her own wallet, the customer is reliant upon an FI to hold her funds and honor contractual obligations in the institution's terms of service. If a dispute arose between a customer and an institution she would rely on records of these agreements to argue her case and achieve satisfaction in a lawsuit. These records would need to show her legal name and physical address at a minimum to prove essential facts in the case. No such reliance or relationship, however, exists between a user who secures her own cryptocurrency credentials and any such third party.

Apart from a reasonable expectation of privacy analysis, the rule's constitutionality is also susceptible from a trespass or "property-based"[122] theory of the Fourth Amendment.[123] We raise these arguments distinctly because the composition of the Court may have recently shifted such that a majority of Justices now believe that *Miller* and *Smith*—the cases that first created a third-party exemption to the warrant requirement—should be "taken off life support" and subsumed within a more traditional trespass theory of the Fourth Amendment.[124] The case on point would therefore be *Ex Parte Jackson*[125] as interpreted in Justice Gorsuch's dissenting opinion in *Carpenter*.[126] *Ex Parte Jackson* deals with the privacy of persons' papers while traveling through the mail. As the Court found,

> The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be.[127]

---

[122] "*Katz* [and the reasonable expectations test] only supplements, rather than displaces the traditional property-based understanding of the Fourth Amendment. [quotations omitted]." *Byrd v. United States,* 138 S. Ct. 1518, 1526 (2018) (internal citation omitted) (quoting *Florida v. Jardines*, 569 U.S. 1, 11 (2013)).
[123] *See generally*: *Carpenter v. United States* (Gorsuch, N., dissenting).
[124] "I do not agree with the Court's decision today to keep *Smith* and *Miller* on life support and supplement them with a new and multilayered inquiry that seems to be only *Katz*-squared." *Id*. at 20.
[125] *Ex parte Jackson*, 96 U.S. 727 (1878), https://supreme.justia.com/cases/federal/us/96/727/.
[126] Justice Gorsuch has no qualms with applying this "ancient" framework to modern technologies. *Carpenter v. United States* (Gorsuch, N., dissenting). ("These ancient principles may help us address modern data cases too. Just because you entrust your data—in some cases, your modern-day papers and effects—to a third party may not mean you lose any Fourth Amendment interest in its contents.").
[127] *Ex parte Jackson* 733.

The Court did not find that this "closure" against inspection need be impenetrable to be worthy of triggering a warrant requirement for search. As the Court held,

> Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles.[128]

A Bitcoin transaction from a self-custodied wallet address is not encrypted; it is plain text and indicates certain facts to the public as an advertising flyer or postcard would when in transit through the mail.[129] These facts, however, are limited to the amounts sent and the pseudonymous Bitcoin addresses that are sending and receiving. The fact of one address's control or ownership by a legal person residing at a physical address is not broadcast on the Bitcoin network nor recorded on the blockchain. Indeed, the deliberate design of the Bitcoin protocol means that this important fact will remain "closed against inspection"[130] as the transaction is broadcast across the network.

Typically, any evidence of an association between a Bitcoin address and a real identity and physical address would exist only within a computer located in the citizen's actual home or on her person.[131] A mandate to obtain that evidence without a warrant is not dissimilar to a mandate that FIs must, on behalf of the government, intrude upon the homes of Bitcoin users transacting with self-custodied wallets and seize private records therein stored. As the Court found in *Kyllo*, it matters not that the intrusion into the home is occurring indirectly by using sophisticated technology or that it is limited to a modicum of private information, or that the information is intimate or mundane—all that matters is that the information sought was secured inside the home:

> [A sophisticated thermal imaging camera] might disclose, for example, at what hour each night the lady of the house takes her daily sauna and bath—a detail that many would consider "intimate"; and a much more sophisticated system might detect nothing more intimate than the fact that someone left a closet light on. We could not, in other words, develop a rule approving only that through-the-wall surveillance which identifies objects no smaller than 36 by 36 inches, but would have to develop a jurisprudence specifying which home activities are "intimate" and which are not. And even when (if ever) that jurisprudence were fully developed, no police officer would be

[128] *Ibid*.
[129] *Ibid.*
[130] *Ibid.*
[131] Examples of such self-hosted Bitcoin solutions include Casa and Start9. See: https://keys.casa/, https://start9labs.com/.

> able to know in advance whether his through-the-wall surveillance picks up "intimate" details–and thus would be unable to know in advance whether it is constitutional.[132]

Irrespective of whether the Court in future cases maintains a *Katz* reasonable expectation of privacy theory of the Fourth Amendment or shifts to a property and trespass theory of the Fourth Amendment, the obligation for banks to search for and seize private information related to the financial lives of persons who are not even FI customers goes significantly beyond the bounds of the Constitution. If the rule is not altered, it will be challenged as a matter of constitutional law and as a matter of our foundational human dignity and right to be left alone.

Forces the Identification and Ongoing Surveillance of Persons Exercising Free Assembly Rights

Another effect of the proposed rule would be to make significant anonymous donations to charitable organizations using cryptocurrency impossible. The proposed rule will obligate financial institutions to keep lists of customers who are members of certain political associations or otherwise associate with certain charitable or public causes whenever they make contributions over $3,000. Paired with the currency transaction reporting rule, this rulemaking will force financial institutions to identify and report every customer who makes a cryptocurrency donation to a charitable organization or political association that is larger than $10,000.

Americans have a constitutional right to assemble anonymously, and laws that mandate the maintenance and reporting of association membership lists have been overturned as violating those rights.[133] In *Shultz*, the Supreme Court was presented with the very fact pattern implicated by this rule: a financial institution was forced to keep lists about the First-Amendment-protected donation activities of its customers.[134] The Court did not offer a judgement as to the constitutionality of those requirements at the time because the defendant, the ACLU, could not show standing and ripeness.[135] This time, however, it will be unequivocal

---

[132] *Kyllo v. United States*, 533 U.S. 27 (2001), https://supreme.justia.com/cases/federal/us/533/27/.
[133] *NAACP v. Alabama*, 360 U.S. 240 (1959), https://supreme.justia.com/cases/federal/us/360/240/.
[134] *Id*.
[135] With respect to the recordkeeping requirement of the BSA, the Court found that "Each of [the successful prior cases vidicating associational rights] was litigated after a subpoena or summons had already been served for the record of the organization, and a action brought by the organization to prevent the actual disclosure of the records. No such disclosure has been sought by the Government here, and the ACLU's challenge is therefore premature." With respect to the reporting requirement, the Court found that "The contentions of the ACLU that the reporting requirements with respect to foreign and domestic transactions invade its First Amendment associational interests are too speculative and hypothetical to warrant consideration, in view of the fact that the ACLU alleged only that it maintains accounts at a San Francisco bank, but not that it regularly engages in abnormally large domestic currency

that the rule demands this sort of surveillance of Americans' protected rights to assemble, and it will be certain that organizations, such as Coin Center, will have standing to challenge the impingement of their donors' Constitutional rights. If this rule is implemented and our donors make contributions to our self-custodied wallet that are greater than $10,000 from regulated hosted wallets, then those transactions will automatically be reported to FinCEN as CTRs, and those donors names will appear in records associating them with Coin Center, the identified counterparty to the transaction, a public advocacy organization.

Sincerely,

Jerry Brito

Executive Director
Coin Center

Peter Van Valkenburgh

Director of Research
Coin Center

transactions, transports or receives monetary instruments from foreign commercial channels, or maintains foreign bank account." *California Bankers Assn. v. Shultz*, 56 and 24-25.