ADAM

ASSOCIATION FOR DIGITAL ASSET MARKETS

January 4, 2021

Via email and www.regulations.gov

The Honorable Steven Mnuchin
Secretary of the Treasury
U.S. Department of the Treasury
1500 Pennsylvania Ave., NW
Washington, DC 20220

Mr. Kenneth Blanco
Director
Financial Crimes Enforcement Network
U.S. Department of the Treasury
2070 Chain Bridge Road
Vienna, VA 22182

Re: Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, Docket Number FINCEN-2020-0020, RIN number 1506-AB47 (the "Rule")[1]

Dear Secretary Mnuchin and Director Blanco,

The Association for Digital Asset Markets ("ADAM") appreciates the opportunity to provide comment on Financial Crimes Enforcement Network's ("FinCEN") above-referenced proposed Rule on unhosted wallets. For the reasons cited below, ADAM believes any final version of the Rule should be amended to address the concerns referenced herein.[2]

The core mission of ADAM is to promote integrity, fairness, and efficiency in digital asset markets and to define and promote ethical conduct by all digital asset market participants. Our members are committed to transparency and protecting market participants from fraud and manipulation, with every member required to adopt and adhere to our Code of Conduct. We are significant stakeholders in the digital asset industry, and appreciate the opportunity to provide comment and FinCEN's consideration of our perspectives.

---

[1] *See* Financial Crimes Enforcement Network's Notice of Proposed Rulemaking: Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, published in the Federal Register on December 23, 2020, and available at: https://public-inspection.federalregister.gov/2020-28437.pdf.

[2] For background, this is ADAM's third letter filed in connection with this rulemaking initiative. *See* letters from ADAM to Treasury filed on December 15, 2020 (requesting that the rule not be Interim Final and instead be a proposal with an opportunity for notice and comment in accordance with the Administrative Procedure Act) and on December 21, 2020 (requesting an extension of the 15-day comment period). For ease of reference, both of ADAM's prior letters – including ADAM's December 15, 2020 letter submitted prior to the Rule release – have been filed electronically via the Federal E-Rulemaking Portal at www.regulations.gov.

I. Summary of the Rule

The Rule proposes to require banks and money services businesses ("MSBs") to submit reports, keep records, and verify the identity of customers in relation to transactions involving convertible virtual currency ("CVC") or digital assets with legal tender status ("legal tender digital assets" or "LTDA") held in unhosted wallets or held in wallets hosted in a jurisdiction identified by FinCEN. FinCEN is proposing to adopt these new requirements pursuant to the Bank Secrecy Act ("BSA").

Specifically, the Rule would require banks and MSBs to file a report with FinCEN containing certain information related to a customer's CVC or LTDA transaction and counterparty including name and physical address, and to verify the identity of their customer, if a counterparty to the transaction is using an unhosted wallet and the transaction is greater than $10,000. The Rule would also require that banks and MSBs keep records of a customer's CVC or LTDA transaction or counterparty, including verifying the identity of their customer, if a counterparty is using an unhosted or otherwise covered wallet and the transaction is greater than $3,000.

II. Significant Process and the Administrative Procedure Act ("APA") Concerns

On Friday, December 18, 2020, FinCEN released the Rule, which was published in the Federal Register on December 23, 2020 with comments due no later than January 4, 2021. For the reasons cited below, the proposed comment period is inadequate.

Under any circumstances, less than three calendar weeks to comment on a rule proposal that could have significant impacts on regulated industries is extraordinary. This notice of proposed rulemaking was released on a Friday just prior to the Christmas and New Year holidays, leaving interested parties a mere eight business days to respond to the 72-page proposal.

ADAM is participating in good faith in the rulemaking process, but the abbreviated comment period has proved to be inadequate for a thorough and informed response to the Rule itself and to the questions FinCEN posed in the Rule, which unfortunately deprives the public of an opportunity for meaningful comment and prevents FinCEN from properly assessing the relative costs and benefits of the Rule pursuant to the cost-benefit analysis requirements for the Rule.

FinCEN cites "national security imperatives" as necessitating an efficient process for proposal and implementation of the Rule, and asserts that notice and comment is not even required in this instance because it would somehow be "impracticable" or "unnecessary." But FinCEN provides no indication of the types of national security concerns that precipitated this rulemaking, let alone how a rule that will inevitably require an implementation period, addresses the asserted concerns. Providing a meaningful comment period would not have threatened national security in any way. To the contrary, a final rule, the impacts of which are not adequately assessed, could pose even greater national security concerns, particularly given recent cybersecurity events and ongoing threats involving the federal government's own information systems. There are many situations in which the government needs to expedite rules for exigent circumstances, but ADAM believes that invoking this critical emergency exception for present circumstances – particularly given the appearance of political motivation and midnight rulemaking – is not well substantiated and weakens the federal government's position when any future exigent circumstances do arise necessitating urgent and critical government action. Treasury is also rumored to have started discussions about a potential rulemaking to this effect in December 2019. If true, there was

no reason to expedite this rulemaking with such a short comment period published in the Federal Register one year later on December 23, 2020.

Further, a 60-day comment period, which would have been in line with other similarly situated rulemakings of this magnitude, would have been more appropriate. In fact, FinCEN and the Federal Reserve Board proposed another BSA rule on October 23, 2020 with a 30-day comment period.[3] The public was not afforded a meaningful opportunity for comment on this Rule, particularly in light of the fact this rulemaking has far more impact, carrying with it a need for thoughtful analysis.

Furthermore, while we understand FinCEN's jurisdiction in this area, it is unclear whether the other financial regulatory agencies were consulted on the Rule. This is of particular importance given the interplay between this Rule and the President's Working Group on Financial Markets (PWG) Statement on Key Regulatory and Supervisory Issues Relevant to Certain Stablecoins released on December 23, 2020.[4] As noted in the PWG's release: "In addition to the Secretary of the Treasury, the PWG includes the Chairman of the Board of Governors of the Federal Reserve System, the Chairman of the Securities and Exchange Commission, and the Chairman of the Commodity Futures Trading Commission. The PWG also sought the views of the Acting Comptroller of the Currency in preparing this statement."[5] We believe a rulemaking of this magnitude, particularly given the interplay with the PWG statement, would benefit from input from all government regulatory stakeholders. ADAM also believes any such rulemaking should be jointly proposed given the cross-jurisdictional impacts (on digital assets, exchange activities, transactions, banking and money services) – take for example, the Volcker rule, which was jointly proposed, and ultimately re-proposed, by all of the federal financial regulators.[6]

---

[3] *See* Federal Reserve Board and FinCEN's Notice of Proposed Rulemaking: Threshold for the Requirement To Collect, Retain, and Transmit Information on Funds Transfers and Transmittals of Funds That Begin or End Outside the United States, and Clarification of the Requirement To Collect, Retain, and Transmit Information on Transactions Involving Convertible Virtual Currencies and Digital Assets With Legal Tender Status, dated October 23, 2020, available at: https://www.fincen.gov/news/news-releases/agencies-invite-comment-proposed-rule-under-bank-secrecy-act.

[4] *See* President's Working Group on Financial Markets' Statement on Key Regulatory and Supervisory Issues Relevant to Certain Stablecoins, dated December 23, 2020, available at: https://home.treasury.gov/news/press-releases/sm1223.

[5] *See* Section 1 of Executive Order 12631, Working Group on Financial Markets, dated March 18, 1988, available at: https://www.archives.gov/federal-register/codification/executive-order/12631.html. Also important to note is the membership crossover between the PWG and the Financial Stability Oversight Council – also underscoring the impact of such a rulemaking and interest from all government regulator stakeholders.

[6] Also, notably, the Volcker Rule was mandated by Section 619 of the Wall Street Reform and Consumer Protection Act of 2010 ("Prohibitions on Proprietary Trading and Certain Relationships with Hedge Funds and Private Equity Funds"). Here, no such Congressional mandate exists instructing implementation of this Rule. It is also unclear to what extent Congress was consulted in this rulemaking. To the contrary, we note that certain members of Congress did weigh in in opposition to the Rule. *See, e.g.*, "Davidson Pens Letter to Treasury on Self-Hosted Wallet Regs," dated December 9, 2020, available at: https://davidson.house.gov/media-center/press-releases/davidson-pens-letter-treasury-self-hosted-wallet-regs. Indeed, if there is widespread support for, and particularly if there are exigent circumstances necessitating, this Rule – it would be implemented in a bipartisan manner with Congressional support.

While we greatly appreciated FinCEN's acknowledgement of ADAM's December 15, 2020 letter, cited in the Rule, we were disappointed to see our letter cited for the notion that industry had provided feedback. Specifically, the Rule states: "FinCEN has engaged with the cryptocurrency industry on multiple occasions on the AML risks presented in the cryptocurrency space and carefully considered information and feedback received from industry participants." ADAM submitted its December 15, 2020 letter in an effort to be proactive based on widespread rumors of rulemaking in an interim final form on social media in the press. In fact, in our letter we expressed ADAM's deep commitment to transparency and concern about the opacity of the process and the content of a potential rule. ADAM respectfully notes that our letter is not evidence of industry feedback – particularly since we were not privy to Rule text prior to release, and instead relied on leaked accounts of potential content.

As noted in our prior letters, ADAM is concerned that this abbreviated comment period circumvents the stakeholders most impacted by these regulations. This potential violation of the APA is a disappointing way to close out the Trump administration's legacy on digital assets, in addition to running counter to the commitment to transparency and fairness that our members promote.

III. The PWG's Statement is a Preferred Approach

On December 23, 2020 the PWG issued the above-referenced statement, noting the following:

> **"To facilitate market integrity,** stablecoin arrangements must meet all applicable AML/CFT and sanctions obligations. Stablecoin arrangements designed to permit anonymous or pseudonymous transactions are likely to attract illicit actors and, without appropriate mitigation measures, allow evasion of key public policy objectives. Like other entities subject to AML/CFT and sanctions obligations, stablecoin arrangements must conduct identification and risk assessment of customers, monitoring of transactional activity, maintenance and provision of records to authorized parties (i.e., regulators and law enforcement) for AML/CFT purposes, reporting of suspicious activity, and screening for sanctions obligations, among other obligations. Before products are brought to market, compliance features must be implemented by the providers subject to AML/CFT requirements within stablecoin arrangements to address these requirements and updated on an ongoing basis as circumstances change. Individual mitigation measures will vary, but they must include an assessment of risk, compliance with all regulatory and supervisory requirements, and effective AML/CFT compliance programs. In addition, stablecoin arrangements ***should have the capability*** to obtain and verify the identity of all transacting parties, ***including for those using unhosted wallets***." (emphasis added)

The statement was released the same day the Rule was published in the Federal Register – and calls for a significant policy measure, which would be an improvement upon and departure from what is set forth in the Rule: "*capability to obtain and verify"* identities is a different standard than the Rule's significant recordkeeping and reporting requirements, and the creation of de facto central repositories mandated by the Rule (for both regulated entities and FinCEN alike). The PWG statement recognizes that regulated entities should be able to reasonably and adequately identify the transaction parties – eg, by using protocol solutions or software like Elliptic or Chainalysis that screens and tracks digital asset transactions to detect and investigate violations and money laundering. There is no de facto requirement for government reporting.

Also of significant importance is that in all likelihood the PWG does not intend to create a double standard for stablecoins. At the very least, FinCEN should re-propose the Rule in light of the subsequent

release of the PWG statement. In fact, the entire Rule should be re-proposed to bring it in line with the policy set forth by the PWG statement, which includes input from five federal government department and agency heads.

IV. Discriminatory Applicability of BSA Standards

FinCEN's Rule contemplates that banks and MSBs subject to the BSA must collect information on the owners of unhosted wallets to or from which those banks and MSBs transmit cryptocurrencies – that is, on the counterparties of their customers. It is critical to note that generally speaking no other bank or MSB subject to the BSA has this kind of obligation. Requiring that virtual asset service providers ("VASPs") collect counterparty information amounts to a new recordkeeping standard that would apply only to certain transactions – a Know Your Customer's Customer ("KYCC") standard. VASPs already conduct KYC, but not KYCC. KYCC requirements in this space would not be technology neutral, which is a foundational principle of financial regulation. In other contexts, banks can apply recordkeeping requirements *based on risk*, while the Rule appears to impose a blanket mandate for such recordkeeping in the case of these transactions.

Underlying the Rule there appears to be an argument linking illicit activity with unhosted wallets. That argument is insufficiently substantiated in the Rule. Available data suggests that the illicit cryptocurrency activity that does take place on exchanges is at the hands of market participants or exchanges with deficient AML controls. Whether adequate AML controls are in place at an institution does not depend on the unhosted wallet ecosystem. When a user at a regulated MSB makes a deposit or withdrawal, that MSB already possesses KYC information on that user in order to serve them. The MSB, if it has appropriate KYC practices in place, can already identify the party who originated the deposit or withdrawal, regardless of what wallet that deposit or withdrawal hit or, respectively, was effected from.

V. Significant Cybersecurity Risks and Privacy Implications

The Rule raises very serious privacy and cybersecurity concerns. Requiring that regulated entities and FinCEN become central repositories of such sensitive information is problematic and must be evaluated further, particularly in light of other rulemakings where similar concerns have been raised warranting rule amendment, or in some cases, withdrawal. ADAM is concerned that while the Rule seeks to address potential illicit finance issues, it instead introduces cybersecurity risks of epic proportions. To the contrary, there have been significant concerns raised by the public and senior government officials alike when proposals are made for the government to become central repositories for sensitive data. Two important examples include the Securities and Exchange Commission's ("SEC") Consolidated Audit Trail ("CAT") and the Commodity Futures Trading Commission's ("CFTC") Regulation Automated Trading ("Reg AT") proposals.[7]

FinCEN should be mindful of the perspectives of the heads of the other financial regulators in similar rulemaking initiatives as they are directly applicable to this rulemaking initiative. CFTC Chairman (then

[7] *See* Statement of Dissent by Commissioner J. Christopher Giancarlo Regarding Supplemental Notice of Proposed Rulemaking on Regulation Automated Trading, dated November 4, 2016, available at: https://www.cftc.gov/PressRoom/SpeechesTestimony/giancarlostatement110416. *See also* Opening Statement of Commissioner J. Christopher Giancarlo before the CFTC Staff Roundtable on Regulation Automated Trading, dated June 10, 2016, available at: https://www.cftc.gov/PressRoom/SpeechesTestimony/giancarlostatement061016.

Commissioner) Chris Giancarlo raised the following cybersecurity concerns in 2016 with respect to Reg AT, which are analogous to issues raised by this Rule:

> "Absent specific measures, it is absurd to suggest that source code will be kept secure. Just look at the area of government cybersecurity. In the six months after the CFTC proposed Reg. AT, hackers breached the computer networks of the Federal Deposit Insurance Corporation and the Federal Reserve. Incredibly, the U.S. Office of Personnel Management (OPM) that gave up 21.5 million personnel records in a year-long cyber penetration failed a security audit last November – six months after the breach was discovered. In fact, federal, state and local government agencies rank last in cybersecurity when compared against 17 major private industries, including transportation, retail and healthcare.
>
> The CFTC itself has an imperfect record as a guardian of confidential proprietary information. If this rule goes forward, the CFTC will make itself a target for a broader group of cyber criminals, including those engaged in commercial espionage.
>
> Last Friday, we learned that a former employee of the Office of the Comptroller of the Currency (OCC) downloaded thousands of files from the agency's servers onto two removable thumb drives without authorization prior to retiring from the agency. The OCC said that when it contacted the former employee about those files, he was 'unable to locate or return the thumb drives to the agency.'
>
> The OCC breach surely sent shivers up the spines of source code owners who received notice that same day of the CFTC's intention to move forward with the Supplemental Notice. They must have been doubly spooked when the CFTC's own servers crashed a few hours later due to a denial-of-service attack."

Any final Rule should address those concerns. There have been multiple government security breaches in recent years, including the recent hack of the Treasury Department's own information systems.[8] FinCEN will not be immune and it will become a target for major national security risks. Furthermore, the Rule will also put the banks and MSBs required to collect the information at risk. For these reasons alone, the Rule should be withdrawn or re-proposed.

Furthermore, CFTC Chairman Giancarlo has noted the extremely dangerous privacy precedent, also of significant concern with this Rule:

> "If the CFTC adopts the source code provisions of the Supplemental Notice, the Securities and Exchange Commission (SEC) will likely copy it and so will other U.S. and overseas regulators – and not just regulators of financial markets. Regulators like the Federal Communications Commission may demand source code for Apple's iPhone. The Federal Trade Commission may seek source code used in the matching engines of Google, Facebook and Snapchat. The National Security Agency may demand to see the source code of Cisco's switches and Oracle's servers. The Department of Transportation may demand Uber's auction technology and Tesla's driverless steering source code. Where does it end?

[8] *See* Reuters: "U.S. Treasury breached by hackers backed by foreign government - sources," dated December 13, 2020, available at: https://www.reuters.com/article/usa-cyber-treasury/refile-exclusive-u-s-treasury-breached-by-hackers-backed-by-foreign-government-sources-idUSL1N2IT0I8.

> It certainly will not end on American shores. Overseas regulators will also mimic the rule...Undoubtedly, this proposed rule is a reckless step onto a slippery slope. Today, the federal government is coming for the source code of seemingly faceless algorithmic trading firms. Tomorrow, however, governments worldwide may come for the source code underlying the organizing and matching of Americans' personal information – their snapchats, tweets and instagrams, their online purchases, their choice of reading material and their political and social preferences. Seriously, where will it end?"

Relatedly, SEC Chairman Jay Clayton, expressed the following concerns with respect to the CAT:[9]

> "The protection of sensitive information submitted to the CAT is of paramount importance, and I share many of the concerns that have been raised about the protection of any investors' personally identifiable information (PII) that would be stored in the CAT...
>
> Make no mistake, even if the SROs significantly reduce the scope of PII included in the CAT, the nature of the data to be included in the CAT necessitates robust security protections. The CAT NMS Plan developed by the SROs includes specific security requirements designed to mitigate the risk of a breach of the CAT and the possibility of misuse of data reported to the CAT. The security features required by the CAT NMS Plan include, among other things: (i) the encryption of PII and all other CAT data, as well as a System Security Plan; (ii) adherence to the NIST 800-53 security standards, a set of security and privacy controls for federal information systems and organizations; (iii) incorporation of tools that will enable logging, auditing and access controls for the CAT system; (iv) secure methods of connectivity; and (v) development of a Cyber Incident Response Plan.
>
> Further, with regard to the use of the CAT by the SEC, as I have previously noted, the SEC will not retrieve any PII from the CAT unless there is a regulatory need for the information and we are confident that there are appropriate protections in place to safeguard the information. Looking ahead, I believe we can and should take additional steps to ensure the security and confidentiality of CAT data, including in response to developments in data systems and cybersecurity. To that end, and recognizing the significant interest in this issue, I have asked the staff to regularly review the security posture of the CAT and advise the Commission if additional amendments to the CAT NMS Plan or other steps are necessary or advisable to further enhance CAT data security."

The SEC has been assessing the CAT for multiple years, partially due to the massive PII and cybersecurity implications involved. How has FinCEN taken into account the sensitivity of such information it seeks to collect under the Rule? What types of information should be removed? What are the security requirements? Will the data be encrypted? What are the access controls? Methods of connectivity? How will the public be made aware of cyber incidents? What are FinCEN's information security standards? How has FinCEN determined that there is a "regulatory need" for such sensitive information for *ALL* transactions over $3,000? This rushed Rule does not answer these questions.

---

[9] *See* SEC Statement on Status of the Consolidated Audit Trail, Chairman Jay Clayton, September 9, 2019, available at: https://www.sec.gov/news/public-statement/statement-status-consolidated-audit-trail. *See also* SEC Statement of Hester M. Peirce in Response to Release No. 34-88890; File No. S7-13-19, dated May 15, 2020, available at: https://www.sec.gov/news/public-statement/peirce-statement-response-release-34-88890-051520 (on liberty and privacy).

With both the Reg AT and CAT, the federal agencies changed their course of action due to the potentially disastrous privacy and cybersecurity implications – only after going through the appropriate notice and comment processes pursuant to the APA. In fact, in the case of Reg AT, the entire rule proposal was later withdrawn.[10]

Indeed, Chairman Giancarlo has also weighed in on his privacy concerns regarding this very Rule, a Rule which is garnering similar negative attention in the press.[11] FinCEN should not ignore these concerns or let them go unaddressed. Unfortunately, the Rule itself raises national security concerns, and ADAM would like to have the opportunity to work collaboratively with FinCEN to help address these issues.

VI. Definition of Unhosted Wallet and Technological Limitations

Another critical issue with the Rule is that it does not define that which it seeks to regulate – there is no definition for "unhosted wallet." The preamble to the Rule characterizes the proposed Rule as a regulation of transactions between wallets hosted by banks and MSBs with "unhosted" or otherwise covered wallets. However, the word "wallet" remains undefined. Thus, the Rule would instead regulate transactions between "customers" of banks and MSBs and counterparties whose "accounts" are not held by a BSA-regulated financial institution or other permitted foreign financial institution. When a "wallet" should be deemed an "account," remains unclear. This is extremely problematic from a compliance perspective. At the very least, given that the entire crux of the Rule is its applicability to "unhosted wallets," FinCEN should re-propose the rule with a definition on which the public can provide comment, particularly prior to any rule going into effect so that banks and MSBs can properly comply. This particular fact also raises its own APA concerns – knowing the definition of "unhosted wallet," *prior to the Rule going into effect*, is important for proper notice and an opportunity for public comment. Furthermore, FinCEN also should not be regulating software on devices, and it is unclear if this is what the Rule intends to do given that unhosted wallets are simply software.

As a separate but related point, the Rule demonstrates insufficient awareness of the practical difficulties that banks and MSBs would have in determining whether their customers' counterparty wallets will be categorized as unhosted wallets. For example, available blockchain analytics tools will have a poor success rate in identifying an unhosted wallet. The Rule does not appear to reflect on these limits of even the best state-of-the-art technology and does not otherwise suggest how a counterparty, when requested to do so by an MSB, would prove that they hold a "private key." Further, the Rule does not address how the identification of an unhosted wallet would proceed in the event that such unhosted wallet is a smart contract. As a practical matter, if institutions do not know how to comply with the new Rule, the only path open to them will be to de-risk their situations by prohibiting the uncertain activity completely, thereby precluding access to the virtual currency markets to many customers.

---

[10] *See* CFTC's Reg AT Proposal Withdrawal, published in the Federal Register on July 15, 2020, available at: https://www.federalregister.gov/documents/2020/07/15/2020-14383/regulation-automated-trading-withdrawal.

[11] *See* Coindesk: Democracy Demands a Say in the Future of Money by J. Christopher Giancarlo, dated December 30, 2020, available at: https://www.coindesk.com/future-of-money-us-treasury-privacy-rights.

VII. Unintended Consequences on Law Enforcement and Compliance

Adopting the Rule in its current form would deprive law enforcement and regulatory agencies of the ability to obtain information that is critical to investigate cases and would make it more difficult for VASPs to engage in risk management. At the present time, the US has a regulatory framework for digital asset exchanges – this allows law enforcement to communicate with VASPs in investigations into customer activity. However, the Rule would interject an unnecessary and complicating factor – namely by creating tensions between the unhosted wallets and the regulated VASPs. There are a variety of potential outcomes that could occur. For example, VASPs may ultimately decide to prohibit any transactions with unhosted wallets, which means that the information about transactions will not be available at the VASPs and therefore making it much more difficult for law enforcement to access these transactions. Alternatively, VASP users could determine not to use the platforms entirely, either to transact wholly by and among unhosted wallets – or use VASPs in jurisdictions with more lax regulatory requirements to engage in digital asset transactions. The effects of this are consequential because transactions would be less traceable and they would receive less monitoring and scrutiny. This amounts to fewer blocking and rejection reports and less information subject to subpoena. Furthermore, the Rule would make risk management for VASPs more difficult as well. This is because unhosted wallet activity could move away from regulated VASPs and therefore provide less information to VASPs, including risk information developed for VASP customers. This means less visibility into the risks VASPs currently monitor and share with law enforcement.

From a practical standpoint, the Rule also amounts to forcing government-mandated inefficiencies into the system. It is highly likely that the Rule would just add a step of withdrawing from a hosted to unhosted wallet of the same ownership before moving any digital assets to other unhosted wallets in the ecosystem. All the Rule does is adds an extra transaction or hop in the transaction chain, which adds additional tracing complexities. No matter where the line is drawn, one more step (to another unhosted wallet) bypasses the artificial barrier. For example, a VASP user in order to move their digital assets would engage in one transaction from the exchange to an unhosted wallet controlled by the VASP user, and then the VASP user can then send it where that user desires to send it. Moving digital assets off the exchange (from custodial wallets) means paying a transaction fee; therefore, the VASP user is incentivized to move everything out at once to avoid higher fees and gain more control over their digital assets. There is no need for regulation to create new steps and barriers.

VIII. Detrimental Impact on Innovation, Competition and US Leadership

Unhosted wallets are foundational to innovation involving blockchain-based systems, including those that involve both financial and non-financial products and services. Restrictions on unhosted wallets would have significant impact on innovation and US leadership in this space – and would most likely force a lot of innovative and productive activity overseas.

From a technology perspective, unhosted wallet software is widely available around the world and usually open-source. This is what enables the self-custody of digital assets. This self-custodial activity means the disintermediation of fee-based middlemen and is the core value proposition of digital assets. Indeed, the ability to transfer digital currencies peer-to-peer is written into the core protocol of nearly every digital asset. The core bitcoin software protocol, for example, is itself open-source non-custodial wallet software, developed collectively by thousands of programmers around the world.

From an innovation perspective, will exchanges stop supporting these transactions? Which companies are going to leave the US? Relatedly, will exchanges engage in their own "de-risking" efforts consistent with Operation Choke Point and fair access? How has FinCEN evaluated these concerns?

Rather than making the US a more attractive place to do business, it will make the US less attractive, for little to no benefit. As a result, while industry participants in the US will be assessing whether the burdens imposed on dealing with unhosted wallets are worth it, the US will lose out to other jurisdictions where industry participants are able to develop more innovative technologies – this would involve, for example, decentralized finance or peer-to-peer smart contracts involving unhosted wallets – at lower costs with less regulatory friction. Also, while other countries have implemented rules for unhosted wallets (eg, Switzerland), those other countries have different legal frameworks and administrative processes. Perhaps we could first seek to take advantage of any lessons learned by those other countries prior to instituting and implementing any new and significant standards in the US – this could be particularly helpful in light of the cost-benefit analysis requirements that exist in the US by providing a basis for assessment of real world impacts. Indeed, most of the laws and rules adopted by other countries are not adopted in the US because of differences in law and policy. By way of example, the US did not implement MiFID, MiFID II, MiFIR – and would not implement such landmark policy frameworks without extensive public consultation.

IX. Insufficient Cost-Benefit Analysis

The Rule would not be effective in achieving its desired outcome yet it would come at a great cost to the public in terms of privacy, liberty and dollars. As a threshold matter, ADAM believes that FinCEN should not dispose of the cost-benefit analysis requirements simply by invoking a "foreign affairs function" and we appreciate FinCEN's implicit acknowledgement in the Rule that all of the cost-benefit analysis requirements do apply.

ADAM, as an industry association, is well-positioned to provide necessary data on the costs of compliance – cost data which FinCEN requests in *11 of the 24 questions for public comment* in the Rule. However, given the time constraints and lack of direct access to such information, particularly on federal holidays, it has proved to be impossible to provide such information. ADAM would welcome a genuine opportunity to provide cost data to FinCEN to enable FinCEN to properly consider the Rule. Preliminarily, the reporting and recordkeeping aspects of the Rule are such that they would amount to a substantial technological build, and would require a significant investment of time from operations and compliance teams – in such a way that would be impracticable to all but the largest firms – and would clash against limitations inherent in what information even the best KYC practices are able to verify from clients.

FinCEN cites, as justification of the Rule's benefits, a report estimating that: "the cost of terrorism globally [was] $33 billion in 2018." ADAM finds it implausible that all transactions over $3,000 are potentially conducted for terrorism purposes. First, only a small fraction of transactions over $3,000 are connected with terrorism or financial crimes. Second, only a small fraction of such transactions are conducted in CVC. As a result, the likelihood that the Rule, even fully and effectively implemented, would prevent a terrorist attack is extremely remote, and the presumed benefit of the Rule therefore infinitesimal relative to the $33 billion figure cited in the Rule.

ADAM is instead concerned about terrorist targeting of FinCEN and the entities forced into compliance with this Rule – there will be serious costs borne by all entities involved. FinCEN has not yet provided the costs it will bear in connection with the Rule's resulting terrorist attacks on the agency, regulated

entities, and costs borne by the public when their information is hacked. Such data could and would be used for a variety of nefarious purposes, but the Rule as proposed ignores these critical concerns.

X. FinCEN Should Consider More Reasonable Regulatory Alternatives that Achieve its Goals

ADAM appreciates the opportunity to supply regulatory alternatives to the Rule, especially as it is unclear which alternatives FinCEN has evaluated. ADAM also welcomes engagement with FinCEN about these regulatory positions, which could potentially achieve FinCEN's goals in a less burdensome, less costly, less intrusive manner while also introducing fewer cyberthreats. Initially, ADAM respectfully requests that the following be explored:

1. First, as the PWG statement notes: "stablecoin arrangements should have the capability to obtain and verify the identity of all transacting parties, including for those using unhosted wallets." The PWG standard regarding *capabilities* should apply in all contexts rather than the Rule's requirements. This would potentially cure most of the problematic issues presented by the current Rule text.

2. FinCEN should also consider the threshold amounts in the Rule. In particular, $3,000 is an extraordinarily low threshold amount in terms of 2021 values. ADAM would welcome assisting FinCEN and conducting a review of appropriate amounts which would potentially be more helpful in achieving FinCEN's goals and make more sense from the public's perspective.

3. The Rule would establish unique reporting and recordkeeping requirements for certain transactions, undermining the principle that financial regulation should be technology-neutral. As noted above, KYCC requirements in this space would not be technology neutral, and ADAM believes a risk-based system for collection of such information would be more beneficial to FinCEN – and more in line with what is required in other contexts. ADAM would appreciate the opportunity to engage with FinCEN to propose metrics and other ways to assess risk, which could then trigger certain requirements. In so doing, this would help minimize the volume of data collected – and FinCEN should also seek to reduce any PII collected.

4. Under no circumstances should FinCEN become a central repository for such sensitive information. While ADAM objects to all of the central repository requirements mandated by the Rule, ADAM believes that at a bare minimum, if these requirements are put in place, any information should be kept by the regulated entities alone.

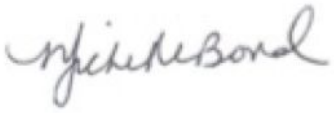
5. FinCEN should first conduct a study prior to engaging in any rulemaking. Perhaps Congress should first mandate a study to more fully understand the risks involved. After receiving input from the study, Congress could then decide what the parameters of any rulemaking should be. Congressional support for any rule would help FinCEN and also be conducted in a bipartisan manner, likely after receiving input from the public.

6. FinCEN should evaluate subpoena authority and consider whether any of its perceived issues can be resolved via existing subpoena authority, or via revisions to its subpoena authority.

Given the profound impact this rulemaking will have on our industry and the public, and the fact that any premature and potentially uninformed issuance of the Rule in final form would harm privacy and national security, and impede continued success of U.S. digital asset market growth, ADAM respectfully

requests that FinCEN: (1) fully withdraw the Rule based on the critical concerns detailed herein and instead conduct a study regarding the issues raised; (2) if FinCEN is unwilling to withdraw, FinCEN should re-propose the Rule by considering all of the regulatory alternatives set forth above and also include the other relevant financial services regulatory agencies in the issuance of any new proposal, especially given their expertise and interests in these areas, and provide a 60-day comment period so that the public can provide appropriate input. Thank you very much for your consideration. We look forward to collaborating further with you.

Respectfully,



Michelle Bond
Chief Executive Officer
Association for Digital Asset Markets (ADAM)

ADAM
ASSOCIATION FOR DIGITAL ASSET MARKETS

ANCHORAGE	BTIG	Genesis	PAXOS
BitGo	CMTDIGITAL	GSR	SARSON FUNDS Real. Clear. Crypto.™
BitOoda	CUMBERLAND A DRW COMPANY	HRT	symbiont
BlockFi	GALAXY DIGITAL	PARATAXIS	XBTO