By Electronic Submission and Email
CC:PA:LPD:PR (REG – 122793 – 19)
Internal Revenue Service
Room 5203,
P.O. Box 7604
Ben Franklin Station
Washington, D.C. 20044

CC: The Honorable Lily Batchelder
Assistant Secretary (Tax Policy)
U.S. Department of Treasury
1500 Pennsylvania Avenue NW
Washington, DC 20220

Re: Comments on Proposed Rulemaking, Gross Proceeds and Basis Reporting by Brokers and Determination of Amount Realized and Basis for Digital Asset Transactions; IRS REG-122793-19

Dear Sir or Madam,

We, the undersigned, appreciate the opportunity to submit comments, and do so via this letter, in response to the Internal Revenue Service's proposed rulemaking REG-122793-19: *Gross Proceeds and Basis Reporting by Brokers and Determination of Amount Realized and Basis for Digital Asset Transaction*s (hereinafter referred to as **'the Proposed Regulations'.**)

While not a formal alliance or association, several companies that create or engage with self-hosted wallets[1] have joined together for this letter to demonstrate their shared concerns regarding the Proposed Regulations. The undersigned includes leading self-hosted wallet providers and developers, who build the relevant hardware and software that enables users to self-host their own wallets, relevant Virtual Asset Service Providers (VASPs), who interact with self-hosted wallets on behalf of their customers in the normal course of everyday business activities, software infrastructure providers that enable self-hosted wallets and others to use blockchain and layer 2 networks, and relevant compliance support companies, such as tax preparation and accounting software firms, who support self-hosted wallet users in complying with applicable tax law.

[1] While we refer to self-hosted wallets within this letter, these types of wallets have also been referred to as 'non-custodial' or 'unhosted' wallets.

Self-hosted wallets enable Americans to secure, control, access, and use their digital assets, whether financial or non-financial. Self-hosted wallets empower all individuals, regardless of economic status, by giving them the tools they need to hold and access their digital assets. As companies involved in the development of self-hosted wallets and services relevant to users of self-hosted wallets, we are proud innovators, leading the development of technologies that enable the digital economy and help to unlock the resulting economic, social, and cultural growth. We significantly and collectively contribute to the American economy, providing not only jobs and economic opportunities, but ensuring everyone has the tools to confidently access and manage their digital lives in an accessible, safe, and secure manner.

We support providing clear rules to ensure that U.S. taxpayers who use digital assets can do so in compliance with applicable law. We appreciate the Proposed Regulations' goals to further provide clarity on the responsibilities of companies and individuals regarding digital asset taxation.

However, as drafted, the Proposed Regulations are overly broad and fail to take into consideration the nuances of the digital asset economy, especially the differences between self-hosted wallets and other service providers that traditionally would be 'brokers'. This results in the Proposed Regulations treating as brokers participants in the digital asset economy that, based on the services and technology they provide, **are not in a position to effectively help U.S. taxpayers and the IRS in digital asset tax reporting.**

As a result, **we have significant concerns that the Proposed Regulations would impose unwieldy, unworkable requirements on these participants** - stifling American innovation, undermining economic empowerment, and creating numerous data and privacy risks, without substantially addressing the concerns of the IRS over tax reporting. Indeed, the Proposed Regulations would significantly increase administrative burdens on the IRS and U.S. taxpayers, resulting in an extraordinary 8 billion new information returns, many of which would be duplicative and unnecessary, and which the IRS has acknowledged that, as of right now, would overwhelm its technology.[2]

[2] IRS Prepping for at Least 8 Billion Crypto Information Returns - Tax Notes, 26th October. Accessed at: https://www.taxnotes.com/featured-news/irs-prepping-least-8-billion-crypto-information-returns/2023/10/25/7hhdp

The Proposed Regulations should be modified so that only those service providers who *directly* effectuate transactions[3] - those that are directly involved in brokering a transaction or involved as counterparty to a transaction - are brokers, and thus subject to the reporting requirements as described in the Proposed Regulations. This will ensure that developers and providers of self-hosted wallets, who do not hold the requisite information, cannot see and are not party to the relevant transactions for reporting purposes, and do not have the same type of relationship with 'customers' as traditional brokers, are properly excluded from being brokers under the Proposed Regulations.

In particular, this letter makes 4 overarching observations:

- ➔ **(1) Self-hosted wallets are not technologically capable of providing the type of information the Proposed Regulations require.**
  - ◆ Below we provide more detail about self-hosted wallets, including what they are for, and the types of information a self-hosted wallet provider sees. Wallets are more akin to a physical, 'leather' wallet that holds a range of real-world credentials, whether that be a library card, an identification document, or a credit or debit card.
  - ◆ As made clear by that description, by their very nature, self-hosted wallet providers and developers cannot comply with the requirements for brokers as set out in the Proposed Regulations because they are not party to covered transactions nor do they have the ability to see the requisite information for reporting.
  - ◆ The most pertinent information for tax reporting purposes, transaction-level data from which gain and loss figures are derived, would remain unavailable to self-hosted wallet providers because they would still not be party to the relevant reporting event, and do not have - and are not required to have - the type of customer relationship that would give them access to this information.
- ➔ **(2) The Proposed Regulations would create, for typical digital asset transactions, redundant categories of multiple brokers, each of whom have the same duplicative reporting requirements on the same transaction, but with access to varying quantities and quality of data, resulting in duplicative, erroneous, and potentially conflicting cost-basis and gross proceeds calculations.**
  - ◆ The broad definitions within the Proposed Regulations would cause there to be multiple brokers with reporting obligations for each transaction, ultimately leading

[3] We use the 'transaction' terminology to align with the Proposed Regulations - e.g. a transaction that results in a taxable event, rather than a non-taxable transaction.

to double, or indeed triple or more, duplicative reports for a typical digital asset transaction.

- Given that self-hosted wallet providers and developers do not hold and cannot see relevant transaction information, requiring them to report would lead to a significant over-reporting for non-disposition events or, alternatively, the need for extensive remediation and reconciliation by taxpayers or the IRS. It would cause significant confusion for taxpayers, the IRS, and compliance-aiding companies (such as tax accounting software firms), ultimately undermining the policy intent.
- Untangling and reconciling the morass of duplicative and erroneous reports will not only be significantly challenging or indeed in some instances impossible, but will greatly increase the compliance burden on taxpayers and the administrative burden and costs on the IRS. The Proposed Regulations do not properly account for the financial impact of these inefficiencies.

➔ **(3) The Proposed Regulations introduce significant privacy and data risks by unnecessarily disseminating personal and financial data to multiple third parties.**

- Many service providers would be required to collect sensitive customer personal data just for reporting purposes, even though they are not otherwise required to do so. This could lead to a wide accumulation and storage of sensitive personal data, offering an opportunity for bad actors to target Americans who simply want to be able to secure and access their assets that enable their digital lives.

➔ **(4) The Proposed Regulations do not promote responsible innovation, representing an analog proposal for a digital age.**

- By not accurately taking into account the purpose, function, or technology of self-hosted wallets, the Proposed Regulations may inadvertently impede the promising and innovative potential of self-hosted wallets. It would, in effect, significantly restrict self-custody, undermining the wider benefits that self-hosted wallets bring, such as consumer protection, economic empowerment, and personal financial and data security for everyday Americans.

We believe significant changes to the Proposed Regulations are necessary to strike an appropriate balance between assisting digital asset taxpayers and fostering responsible innovation. We welcome the opportunity to share our position and expertise and stand ready to further engage on the Proposed Regulations.

Discussion and Recommendations

Section 1: Self-Hosted Wallets - Technical Principles and Key Benefits

As written, we do not believe the Proposed Regulations accurately take into account the nature or purpose of self-hosted wallets. Self-hosted wallets are software or hardware solutions, more akin to a physical, leather wallet that holds a range of important credentials, whether a local library card, an identification card, or credit or debit cards that enable the user to access funds. Like producers of these physical wallets, developers and providers of self-hosted wallets do not have, and are not required to have, the same type of customer relationships with users as do traditional financial services providers. Rather than 'customers,' as described in the Proposed Regulations, self-hosted wallet providers have users who license their software or purchase their hardware. This is not analogous to banks that issue the debit and credit cards and hold the underlying accounts for their customers. It is those financial services providers that have relevant transaction information because of their relationships with their customers, clearly classifying them as 'brokers'. This is not true for providers of self-hosted wallet software or hardware.

As the Bill was drafted, many members of Congress sought to address and clarify the scope of drafting, acknowledging the potential for a wider interpretation than was intended. We draw attention to the Congressional record between Senator Portman, and Senator Warner, where Senator Portman sought to confirm that the provision applied to '***a sale on behalf of someone else***', and did not apply to '***hardware and software sellers for digital wallets***'. Senator Warner confirmed that this was Congress' understanding of the provision.[4] We believe Congress' clear focus on intermediated, third-party sales, and its specific differentiation of wallets from that category, makes plain that the IRS must carefully re-consider the Proposed Regulations.

Before providing our thoughts on the specifics of the Proposed Regulations, we provide technical details of how keys and blockchains work; how self-hosted wallets fit into this technology; and the critical benefits of self-hosted wallets for users and the wider digital ecosystem. This will help demonstrate that consistent with the fundamental difference in the type of service provided to traditional 'brokers', providers of self-hosted wallets are not a party to relevant transactions, nor have the technological ability to acquire the types of information useful to the IRS.

---

[4] https://www.congress.gov/congressional-record/volume-167/issue-144/senate-section/article/S6061-7

Blockchains, Keys, and Wallets

A common misunderstanding is that digital asset wallets (custodial or self-hosted) hold digital assets. They do not. Digital assets cannot leave the blockchain on which they are issued. At its most simple, a blockchain is simply a distributed ledger that tracks which assets are associated with which addresses. A transaction on a blockchain is an instruction to update the ledger to reflect that a given asset formerly assigned to one address should now be assigned to another.

Thus, a digital asset wallet simply holds a blockchain address, which consists of a key pair, made up of two parts: a public address and a private key. Both parts of this key pair are cryptographically derived strings of random characters. The public key generates an address that can be safely shared with others, allowing others to ‘find’ the owner of the address in question - it is equivalent to a phone number listed in a directory that people can be given to call (or indeed send an asset to). The private key is all that is necessary to access and control assets assigned to a particular public address. These keys provide the essential link between an owner and the blockchain address containing their assets.

A hardware or software wallet, therefore, does not contain digital assets, but instead stores the private keys that allow access to digital assets attributed to the corresponding public blockchain addresses. In this sense, a wallet is more accurately thought of as a 'signing device' or, as described above, a physical wallet that holds credentials like a credit or debit card that allows a user to access to assets but is not itself the asset, or holding the asset.

Hardware and software wallets, while popular, are not necessary to hold private keys. Some users opt instead to simply memorize the key (a 'brain wallet'), write it down on a scrap of paper (a 'paper wallet'), or engrave it into some physical medium (a ‘titanium wallet’). Any of these methods is equally a 'wallet.' Hardware and software wallets are popular because they offer advantages in terms of security and convenience.

What is a self-hosted wallet, and how do they work?

As described above, hardware and software wallets store private keys. Private keys, because they control the access and use of digital assets, are extremely important to keep secret: anyone with access to them will have access to the assets associated with them. Users will often hold their digital assets in multiple blockchain addresses for security reasons - resulting in multiple private keys to store and manage.

Generally, there are three types of self-hosted wallets:

- ➔ **Software Wallets**: A software application that stores private keys within an interface that is always connected to the internet.
- ➔ **Hardware Wallets**: Hardware that stores private keys offline in a secure physical device, isolated from an internet connection. Hardware is often a portable device that plugs into a computer or interfaces with an app to sign a transaction with the required keys.
- ➔ **Paper or Other Physical Wallets**: Private keys written on a printed piece of paper or written on other physical medium (e.g. etched onto durable metal such as titanium), retrieved as needed to use the keys. They are less common given concerns over durability and ease of use.

For most people, using a paper wallet or other non-specialized solution to track many private keys is not practical: in raw form, a private key is a 256-bit number, or a random, 78-digit string of numbers, which would need to be manually entered to be used each time. Before the creation of specialized software and hardware self-hosted wallets, early users manually managed keys with complex, insecure, and easily lost spreadsheets. As a result, many people 'misplaced' their private keys, and accordingly lost access to significant amounts of digital assets.[5]

A self-hosted wallet - a hardware or software solution that allows access and management of digital assets stored on the blockchain - is an easier and safer way for users to keep and manage their (potentially unlimited) private keys. It automates and creates user-friendly methods to secure private keys and use digital assets, including, for example, automated key backup functionality to prevent loss. Self-hosted wallets are similar in intent (although not approach) to a password manager: they secure, encrypt, and enable user-friendly access to a multitude of complex passwords. Like password managers, these self-hosted wallets do not see, handle, or direct user activities on relevant websites.

With a self-hosted wallet, the user is entirely responsible for securing, managing, and using their private keys, and therefore is solely responsible for how they access blockchains and blockchain protocols, and their control and use of their digital assets. When a self-hosted wallet user 'creates' a new blockchain address, the blockchain protocol cryptographically generates the key pair which is stored inside the wallet

[5] E.g. the case of James Howells, who accidently threw away a harddrive containing his private keys into a municipal dump in Wales, rendering around 8,000 bitcoins inaccessible. See: https://www.newyorker.com/magazine/2021/12/13/half-a-billion-in-bitcoin-lost-in-the-dump

software run on the user's computer or browser or the user's hardware wallet device or hardware - the key pair is not assigned by and never known to the wallet provider.

This is in contrast to a 'custodial' wallet, in which a digital asset owner transfers their digital assets from a blockchain address they control (by holding the private key) to one controlled by a third-party intermediary. 'Hosted' wallets are commonly omnibus accounts, in which assets belonging to multiple owners are commingled in one or more blockchain addresses and accounted for 'off-chain' in the custodian's internal books and records. The beneficial owner of such commingled assets gives up direct access and control, and instead must rely on the host platform to carry out their wishes (akin to directing a bank to transfer fiat currency across accounts).

Because of how self-hosted wallets operate, self-hosted wallet providers and developers do not and are unable to know the details of any particular taxable transaction conducted by a self-hosted wallet user. Unlike custodial platforms, self-hosted wallet providers do not perform, execute, or 'effectuate' transactions on behalf of users. As a result, self-hosted wallet providers will often partner with third-party service providers, such as digital asset exchanges or platforms, to ensure users have a secure and seamless experience of moving digital assets between their exchange accounts and their self-hosted wallets.

These partnerships often focus on simply allowing a user to connect their self-hosted wallet to an exchange with which the user has an account, accomplished by the self-hosted wallet having one or more integrations through exchange Application Programming Interfaces (APIs). In these arrangements, the purchase or sale of digital assets is effectuated and made by a digital asset exchange, and the transfer of digital assets to or from a self-hosted wallet is done as a separate action by the user - subject to transaction withdrawal policies managed by the custodial platform or exchange (even if made simpler by an API). Both actions are, ultimately, customer-directed and are completely separate transactions. Self-hosted wallet providers therefore do not have information about relevant transactions, such as whether a purchase or sale transaction is related to a transfer, who the counterparty to a separate transaction may be, or other relevant information such as cost basis, gross proceeds, or the date and time of any disposition.

In many ways, a self-hosted wallet in this scenario is extremely similar to an internet technology company that functions as both a search software provider and a hardware provider. Google or Microsoft provide branded laptops and smartphones; app stores or

search interfaces to find and access relevant financial services providers; and branded storage devices (for example, a hard drive) that customers may use to hold passwords and card information for financial services accounts 'offline'. However, neither company would have involvement in or knowledge of any particular sale of securities, nor be required to report it (a point that the IRS has recognized in other tax regulations). We discuss this question in more detail later in the letter.

The best way to think of a self-hosted wallet is, ultimately, as a wallet: it holds financial services credentials - such as a debit or credit card - which holders use to 'unlock' their financial services accounts, and it can also hold other documents, whether that be a form of identification like a drivers license, insurance cards, or a treasured picture of a loved one. Self-hosted wallets allow Americans to carry their digital assets safely and securely in the digital age.

Self-Hosted Wallet Benefits

As a secure means of access to manage digital assets on the blockchain, self-hosted wallets have several important benefits. While these have been discussed in greater depth elsewhere[6], and the focus of our comments is on the Proposed Regulations, we nonetheless wanted to highlight two benefits that could be lost if self-hosted wallet services are made unviable:

- **Reducing counterparty risk, therefore providing important consumer protections**;
    - With a self-hosted wallet, customers control their digital assets by securing and maintaining direct access to the private keys. This is in contrast to a custodial wallet, where customer digital assets are often held as 'balances' on an internal ledger rather than as a property right to a digital asset on the blockchain. In the event of a financial crisis, bad governance, or bankruptcy of that exchange or platform, there is a high risk that a customer would not have access to their assets.
    - Self-hosted wallets provide consumer protection, ensuring users can interact easily with exchanges but remain ultimately responsible for, and in control of, their digital assets.
- **Security of personal data and prevention of financial loss for users.**

[6] For example, The Blockchain Association's *Self-Hosted Wallets and the Future of Free Societies* (https://theblockchainassociation.org/wp-content/uploads/2020/11/Self-Hosted-Wallets-and-the-Future-of-Free-Societies.pdf)

- With a custodial or exchange-hosted wallet, the keys are often kept on a central server, and retrieved to perform necessary instructions for customer digital assets. Not all exchanges or custodial platforms invest in the same level of security. Like any centralized server, this represents a digital risk, which may be compromised by hackers or bad actors.
- Self-custody introduces an additional level of system-wide security by holding them on secure hardware or software. This not only ensures a customer can effectively prevent bad actors from gaining a full picture of their total assets (a risk from the Proposed Regulations we discuss later) but makes it easier for users to properly hold their keys safely and securely, without the related risk of loss of other forms of holding.

Section 2: Proposed Regulations and Self-Hosted Wallets: Specific Impacts

Overview - Requirements for Self-Hosted Wallets, and Comments on General Principles of Regulations

Before proceeding to specific concerns, we wanted to make some general comments on the principles behind the Proposed Regulations, and how these would unnecessarily cover self-hosted wallets.

As with other brokers that would be covered by the Proposed Regulations - including Virtual Asset Service Providers (such as custodial exchanges), digital asset payment processors, and digital asset kiosks - '*digital asset middlemen*' would be required to undertake three core functions:

- ➔ Tax Reporting via form 1099-DA.[7]
  - ◆ This form includes personal customer information (such as Full Taxpayer Name, Taxpayer Identification Numbers, and Taxpayer Address), transaction details (such as gross proceeds, sale date and time), and relevant transfer information (such as wallet addresses involved).
- ➔ Cost-basis tracking and transfer.[8]
  - ◆ Brokers would be required to track cost-basis on new digital asset acquisitions, and additionally share this information with one another when assets are transferred.

[7] Proposed Regulations (https://www.federalregister.gov/d/2023-17565/p-103)
[8] Proposed Regulations (https://www.federalregister.gov/d/2023-17565/p-127)

- ➔ Tax withholding.[9]
  - ◆ Where appropriate and required, such as where an incorrect TIN is furnished, brokers would be required to undertake relevant tax withholding activities to ensure appropriate tax collection on covered assets.

The Proposed Regulation's definition of a 'digital asset middleman' is uniquely broad:

- ➔ '*any person who provides a facilitative service… with respect to a sale of digital assets wherein the nature of the service arrangement is such that the person ordinarily would know or be in a position to know the identity of the party that makes the sale and the nature of the transaction potentially giving rise to gross proceeds from the sale'*. [10]

In turn, the Proposed Regulations suggest there are three aspects required to be defined as a digital asset middleman:

A. Facilitates: Provides '*a service that directly or indirectly effectuates a sale of digital assets*'.[11]
B. Identifies: Either can, or could have the ability to change the software to be able to, '*request that the party making the sale provide that party's name, address, and taxpayer identification number*'. [12]
C. Transaction Visibility: Either can, or could have the ability to, '*determine whether and the extent to which the transfer of digital assets involved in a transaction gives rise to gross proceeds*' [13]- for example, if software can '*change the fees charged for facilitative services*', it is deemed to be in a place to be able to know transaction details.

We believe this definition is overly broad, capturing parties that would not be brokers in comparable financial transactions elsewhere. For example, the standard reporting requirements in other parts of the Code and regulations more usually focus on those who '*know or has reason to know*': something that is an inherent part of the service offered, usually with the requirement that a broker has a sufficiently direct relationship with its

---

[9] Proposed Regulations (https://www.federalregister.gov/d/2023-17565/p-152)

[10] Proposed regulation, Section 21 - https://www.federalregister.gov/d/2023-17565/p-851

[11] This includes 'providing access to an automatically executing contract or protocol, trading platform, automated market maker system, order matching service, service to discover the most competitive buy and sell prices, or escrow service ensuring that both parties to a sale perform under their obligation' - https://www.federalregister.gov/d/2023-17565/p-854

[12] https://www.federalregister.gov/d/2023-17565/p-71

[13] https://www.federalregister.gov/d/2023-17565/p-71

customer to be considered an entity that has the requested information. **Instead, these Proposed Regulations extend this to some broader set of service providers that are 'in a position to know' this information, arguing effectively that anyone who *theoretically could, must report*, regardless of the technical realities.**

Overly Burdensome

In any case, the Proposed Regulations represent an extremely burdensome and, in many cases, an economically impractical *and often impossible* requirement for self-hosted wallet providers, one that the IRS has begun to acknowledge in its analysis of the economic impacts:

'Start-up costs are estimated to be between three and eight times annual costs... we estimate per firm start-up aggregate burden hours to range from 1,275 to 3,400 hours and $81,000 to $216,000 of aggregate monetized burden. Using the mid-points, start-up total estimated aggregate burden hours is 11,804,375 and total estimated monetized burden is $749,925,000.' [14]

Whilst already representing a large cost, these are nonetheless a significant underestimation for self-hosted wallet providers and developers, who have *never* been required to undertake the proposed information collection and reporting roles, given that their relationship to customers is a software service provider who licenses software to a user or as a seller of hardware, not as a traditional financial service broker that effectuates taxable transactions. This is compounded by the 'start-up' nature of many self-hosted wallet providers - many are innovative, smaller players who would struggle with highly burdensome and costly new rules. Self-hosted wallet providers would need to consider carefully their business models and whether their services are impractical or impossible in the United States.

Detail of Issues

- ➔ **(1) Self-hosted wallets are not technologically capable of providing the type of information the Proposed Regulations require.**

The Proposed Regulations posit that self-hosted wallets effectuate transactions, and are therefore brokers, by virtue of being 'digital asset middlemen'. However, this logic is not based on the reality or purpose of self-hosted wallets, which **do not effectuate**

[14] https://www.federalregister.gov/d/2023-17565/p-326

transactions or have access to relevant transaction data by their very nature. The Proposed Regulations are therefore unworkable, creating a category of brokers that *cannot* perform the task required of them.

A self-hosted wallet, as outlined in the technical explanation above, does not undertake relevant taxable transactions and does not hold assets, but instead is a hardware or software solution that allows a user to access and manage digital assets stored on the blockchain. It cannot transfer assets on the user's behalf, as a 'custodial' wallet does when directed. It is only the user - or the 'self' in the self-hosted wallet - that moves their assets using the blockchain, and whom remains in sole control of their digital assets.

These technical realities are acknowledged by the Proposed Regulations:

- '*in general, only the user of an unhosted* [self-hosted] *wallet has access to both the public and private keys necessary to effect transactions in the digital assets associated with those keys*'.[15]

The Proposed Regulations additionally outline how the 2021 Infrastructure Investment and Jobs Act (IIJA) sought to define a broker:

- '*section 80603(a) of the Infrastructure Act clarifies the definition of broker to include any person who, for consideration, is responsible for regularly providing any service effectuating transfers of digital assets on behalf of another person*'. [16]

Taken together, the IIJA definition and the Proposed Regulation's *acknowledged* reality of a self-hosted wallet's role provide a clear logical inconsistency: only the *user* of a self-hosted wallet can effect transactions, but regardless, a self-hosted wallet is a digital asset middleman and therefore a broker because *it* effectuates transfers as defined under the IIJA. Indeed, not only is a self-hosted wallet not party to any relevant transactions - which are done separately on an exchange or other platform - but the very logic of the Proposed Regulations accepts the role of the user in self-effectuating, undermining the case that a self-hosted wallet can effectuate the transaction and be considered a broker.

[15] https://www.federalregister.gov/d/2023-17565/p-12
[16] https://www.federalregister.gov/d/2023-17565/p-33

Self-hosted wallets do not effectuate transactions in the first instance, and the Proposed Regulations further concede that self-hosted wallets *do not even see* the transactions in question to be able to report them.

As part of the Proposed Regulations, a broker must know the intention of a transfer to be considered effecting a transaction, and therefore subject to reporting:

- *'The definition of effect in proposed §1.6045–1(a)(10) limits the sales for which such brokers must make a report to those transactions in which the broker (as agent) would ordinarily know the gross proceeds from the sale or (as digital asset middleman) would ordinarily know or be in a position to know the identity of the party that makes the sale and the gross proceeds from the sale.'* [17]

Given this requirement, the Proposed Regulation correctly identifies that in Peer-to-Peer (P2P) transactions, the broker will not know the intention, and therefore is not required to report:

- *'In certain circumstances, a digital asset broker... might transfer digital assets without knowing that the transfer was part of a sale transaction. For example, a customer might direct such a custodial broker to transfer digital assets to the wallet of a merchant in connection with the purchase of goods or services from that merchant.*

  The custodial broker in this example... is not in a position to know that the transfer was associated with a sale or exchange transaction or the amount that the customer received as gross proceeds from the exchange (that is, the amount the customer received in consideration for the digital assets surrendered).

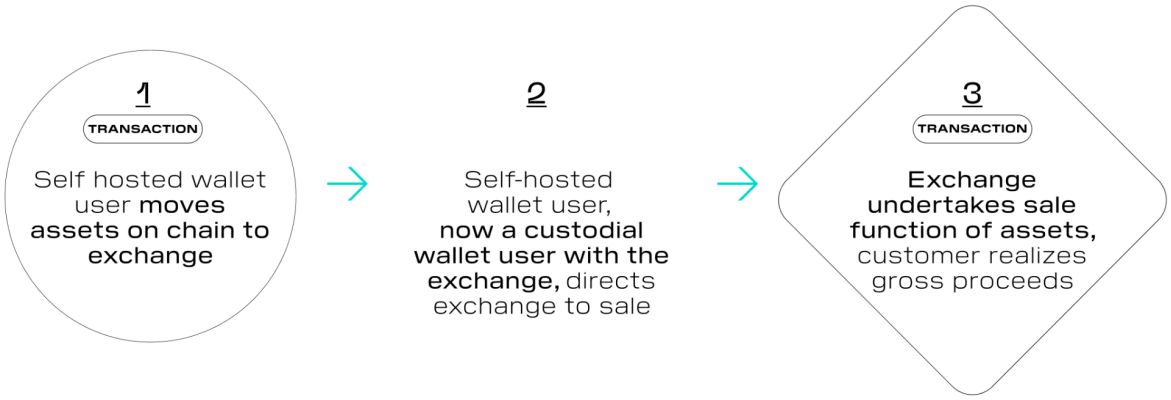
  Accordingly, the transfer of digital assets by that custodial broker to the wallet of the merchant does not constitute effecting a sale of digital assets by that broker.' [18]

Whilst the example specifically references a custodial broker situation, the underlying logic applies to self-hosted wallet transactions – not merely in a particular P2P instance but more generally to all transactions initiated by a self-hosted wallet user. Not only would a customer not 'direct' a self-hosted wallet provider, and putting aside for a

[17] https://www.federalregister.gov/d/2023-17565/p-95
[18] Ibid.

moment the reality that a self-hosted wallet provider cannot see the transaction, there is no way in which a wallet provider could even *know* what the transfer is associated with, or the amount the customer received if there was a relevant tax-related transaction.

To further illustrate, we draw attention to the typical transfer of digital assets using a self-hosted wallet to a centralized exchange–a common type of transfer given that 75% of funds from personal wallets are sourced from exchanges and 64% arrive from for disposition or use.[19] The steps taken to realize any gross proceeds is an entirely separate and secondary transaction that occurs *after* the asset has moved 'on-chain' to the exchange. The causal diagram can be seen as thus:



The self-hosted wallet provider, as a threshold matter, does not itself have information about the user's transaction because that transaction is self-effectuated. Moreover, the self-hosted wallet provider would have no insight into what is being done with the digital assets: it has no information about the purpose of the transaction, such as whether the transfer was done to, later in the transaction chain, purchase an espresso or to exchange digital assets for another currency.

As described by Treasury Assistant Secretary Davidson in February 2022, it is the '*Treasury Department's view that ancillary parties who cannot get access to information that is useful to the IRS are not intended to be captured by the reporting requirements for broker.... existing regulations impose broker reporting obligations only on market participants engaged in business activities that provide them with access to information about sales of securities by taxpayers*'[20]. As self-hosted wallet providers or developers do not have access to this information, they should not be subject to the requisite

[19] Regulations.gov, Chainalysis Comment Treasury Illicit Financing in Digital Assets RFC, 3 November 2022, page 32: https://www.regulations.gov/comment/TREAS-DO-2022-0018-0066

[20] https://www.stradley.com/-/media/files/publications/2022/02/crypto-davidsonletter.pdf?la=en&rev=b70305b1549241499395d19f03d4b32e&hash=72BF0360EABE4BC8EACCB8198F51371C

reporting requirements, and requiring them to do so would make brokers who cannot undertake the requirements made of them.

This key point is recognized in international standards, such as the Organisation for Economic Co-operation and Development (OECD) Crypto-Asset Reporting Framework (CARF), which rightly does not impose tax reporting obligations on self-hosted wallets, instead arguing that: *'those Entities or individuals that as a business provide services effectuating Exchange Transactions in Relevant Crypto-Assets, for or on behalf of customers... are expected to have the best and most comprehensive access to the value of the Relevant Crypto-Assets and the Exchange Transactions carried out.... [and are] considered Reporting Crypto-Asset Service Providers'.* [21]

- ➔ **(2) The Proposed Regulations would create redundant categories of multiple brokers, each of whom have the same duplicative reporting requirements on the same transaction, but with access to varying quantities and quality of data, resulting in duplicative, erroneous and potentially conflicting cost-basis and gross proceeds calculations.**

We have established that the Proposed Regulations would create a class of self-hosted wallet brokers who are not a party to the relevant transactions, and cannot by their nature provide the information requested. If the regulations proceeded, and self-hosted wallets were required to even attempt to comply, the outcome of the Proposed Regulations would be to create onerous and duplicative reporting requirements. Multiple 'brokers' would be required to file *the same information,* and would inherently do so with incomplete, inconsistent, and conflicting data points that would require significant and sometimes impossible reconciliation and remediation by the IRS. This is an impractical regulatory burden that does not achieve the IRS's stated goals.

The Proposed Regulations acknowledge the risk of duplicative reporting, but do not, as might be expected, seek to clarify which brokers should report, failing to add to the list of exempt recipients '*under the multiple broker rule of existing §1.6045–1(c)(3)(iii), which exempts brokers who conduct sales on behalf of other brokers, [so that] only the broker that has the closest relationship to the customer is required to report information'*. [22] This problem is further exacerbated by there being no 'de minimis' threshold, and the requirement for reporting on a per transaction basis.

---

[21] https://www.oecd.org/tax/exchange-of-tax-information/crypto-asset-reporting-framework-and-amendments-to-the-common-reporting-standard.pdf

[22] https://www.federalregister.gov/d/2023-17565/p-80

This onerous requirement has the potential to overwhelm the tax system and taxpayers, with the IRS reporting that it expects 8 billion information returns, representing twice as many information returns as all other 1099 forms combined.[23] Individuals and entities would find themselves inundated with multiple, duplicative reports for the same transactions, resulting in the need to file extensive paperwork for each transaction. This not only strains compliance efforts but also imposes an unnecessary administrative burden on U.S. taxpayers, contrary to the spirit of new regulations. Furthermore, this approach makes it more challenging for the IRS to efficiently verify the reported information. Instead of working with those who actually deal with the relevant transaction, the IRS would instead be required to reconcile multiple copies of competing transaction reports.

For self-hosted wallet providers, this information is, despite best efforts and intentions, likely to be incomplete or materially different from that submitted by the actual transaction broker. As detailed above, self-hosted wallets do not see transaction data or know transaction intent, or are '*not in a position to know that the transfer was associated with a sale or exchange transaction or the amount that the customer received as gross proceeds from the exchange'.* [24]

There are therefore two outcomes that the IRS is asking for here, both of which are undesirable. The IRS may be asking for self-hosted wallet providers to guess the information required, presuming and reporting that, for consideration, the full amount was disposed of instantly at the current fair market value, even though, as a separate transaction to which the self-hosted wallet providers is not party to, this information is unverifiable. Alternatively, the IRS may be asking for self-hosted wallet providers to request the relevant exchange or platform for the information so that they can report in parallel with the entity in question on form 1099-DA. In both situations, the IRS is asking for an unnecessarily duplicative process that does not increase confidence in the reporting. Either self-hosted wallet providers are being forced to batch report using limited and unverifiable data, or they are being asked to performatively comply with the regulations and report *others' information*, with no ability to determine whether this is indeed correct.

Left with no choice but to issue at the very least 'best-estimate' 1099-DAs for each and every transaction to ensure 'blind' compliance, self-hosted wallet providers would have

---

[23] IRS Prepping for at Least 8 Billion Crypto Information Returns - Tax Notes, 26th October. Accessed at: https://www.taxnotes.com/featured-news/irs-prepping-least-8-billion-crypto-information-returns/2023/10/25/7hhdp

[24] https://www.federalregister.gov/d/2023-17565/p-95

to issue a huge number of unnecessary reports to customers, some of which do not actually report a covered transaction. In turn, the IRS would need to do significant remediation and reconciliation work to match these reports to the *actual* reports from those brokers with knowledge of the disposition to understand which transactions fall into scope. The same is true for tax-compliance companies, who would struggle to disentangle actual dispositions from 'blind' estimates.

In either situation, taxpayers are furnished with unhelpful, confusing tax data. Given the lack of a de minimis threshold, they would receive such a statement potentially for each and every transaction they undertake: whether that be purchasing a large shot of espresso, or disposing of assets for a significant fiat sum. The sheer amount of paperwork would understandably overwhelm even the most seasoned of tax veterans, and not provide the IRS with the data it wants to make enforcement decisions.

The IRS has already indicated the Proposed Regulations would result in an extraordinary 8 billion information returns, many of which would be duplicative and unnecessary reports.[25] These proposals do not make the tax system easier, faster, or simpler, not least because of the onerous duplicative reporting requirements. As acknowledged in the Proposed Regulations, *'avoidance of duplicative reporting is... a desirable goal for digital asset reporting*'. We firmly agree, and encourage the IRS to do so by ensuring that only the actual broker to a transaction - that which directly effectuates a covered transaction - is subject to the requirements outlined.

➔ **(3) The Proposed Regulations introduce significant privacy and data risks by unnecessarily disseminating personal and financial data to multiple third parties.**

The Proposed Regulations fail to take steps to appropriately protect taxpayer data safety, unnecessarily disseminating personal and financial data to multiple third parties, creating a perverse incentive structure that will encourage bad actors to seek to exploit these 'honeypots'.

At present, the Proposed Regulations require each form 1099-DA to be furnished with the following information[26]:

- The U.S. taxpayer's name, address, and taxpayer identification number

[25] IRS Prepping for at Least 8 Billion Crypto Information Returns - Tax Notes, 26th October. Accessed at: https://www.taxnotes.com/featured-news/irs-prepping-least-8-billion-crypto-information-returns/2023/10/25/7hhdp
[26] https://www.federalregister.gov/d/2023-17565/p-103

- The name, type, number, date, and time of digital assets sold
- Gross proceeds the seller received from the sale
- Gross proceeds from using digital assets to pay trading fees to the broker
- Wallet address(es) from which a digital asset was transferred as part of the sale
- The transaction identification or hash associated with the sale, where the sale or transfer into the customer's account occurs on-chain

This is a wide range of extremely sensitive personal information. It is commonly understood that personal names, addresses, and taxpayer identification numbers are some of the most sensitive and important information that U.S. taxpayers possess. The utmost priority should be placed on ensuring that these details are only collected where necessary, and where they can be securely stored in a *knowable* number of institutions. This is part of the reason why it is correctly stated that '*avoidance of duplicative reporting is... a desirable goal*'.

However, and more uniquely for these regulations, the collection and reporting of user data linked to wallet addresses introduces a level of risk that is concerning in the context of digital transactions. In particular, it risks exposing the history of transactions of identified individuals in a way that is fundamentally different from traditional finance, and will lead to real-world implications for individuals.

A wallet address, once the holder is known, provides a unique insight into the assets held, providing a full picture of an individual's finances. As acknowledged by the Treasury - in its illicit finance risk assessment of Decentralised Finance - '*The transparency of blockchains complicates attempts to move or obfuscate funds even pseudonymously. Financial institutions, regulatory agencies, and law enforcement may use multiple complementary third-party tools to identify, trace, and attribute virtual asset transactions on most virtual asset blockchains.*' [27]

Therefore, if you know a wallet address, you can see the specifics of the assets held within, and the transactions associated with it. Digital asset users therefore rightly take steps to protect this data, given that nobody would want their personal bank account or credit card transactions to be readily visible to any actor in society. This is a unique feature of the distributed ledger system. Regulations should not seek to merely cross-apply traditional approaches to digital finance, but update them to best reflect the function of the technology.

---

[27] https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf

Courts have begun to acknowledge the unique features and particular implications of the blockchain. In June 2023, for example, '*US Bankruptcy Judge John Dorsey agreed to... redact the names of the 50 biggest unsecured creditors owed a total of $3.1 billion. The US Bankruptcy Code normally requires the names be filed in documents available to the public.*' [28] Judge Dorsey acknowledged that '*It is the customers who are the most important issue... we want to make sure that they are protected and they don't fall victim to any types of scams*."[29] The judge did this because unmasking wallet addresses - and linking them to real-world identities - is a particular risk of the blockchain that must be addressed when taking action.

We posit therefore that wallet addresses should be considered, in the instance of digital asset reporting, to be as valuable personal information as taxpayer identification numbers. Combining wallet addresses and personal sensitive data, and ensuring this information is by regulation spread across multiple parties to a transaction could inadvertently create a 'honey-pot' scenario, divulging critical information about who controls which wallet and the respective holdings within, as well as a 'real world' link via addresses and TINs.

By requiring multiple parties to hold this data (even when they do not otherwise have a legal obligation to do so), the IRS could inadvertently create a 'real world' profiling and targeting resource for bad actors, and the risk of this has been significantly understated by the regulations. In the event of a breach, a leaked database under this proposed rule would provide a comprehensive list of targets, their locations, and the extent of their cryptocurrency holdings.

Recent incidents have demonstrated the significant losses that users - even without relevant wallet addresses attached - can face due to phishing attacks and cybercrime. A good example is the Equifax data breach, which saw the sensitive personal data of 148 million people compromised, including names, addresses, and social security numbers. [30] Had this included wallet addresses, the damage could have been greater. Not only would having such addresses exacerbate the already existing risk of online remote scams, but they can also lead to what has been termed '$5 wrench attacks'.[31]

---

[28] https://www.bloomberg.com/news/articles/2022-11-22/-substantial-ftx-assets-are-stolen-or-missing-attorney-says?sref=noeqZDPr

[29] https://www.reuters.com/legal/ftx-customer-names-will-not-be-revealed-by-bankruptcy-court-2023-06-09/

[30] https://www.equifaxbreachsettlement.com/

[31] E.g. Dentzel Zaryn was tortured at home in Spain to give up his private keys, after assailants were able to trace his finances across wallets (https://www.financemagnates.com/cryptocurrency/news/gang-attempted-to-steal-bitcoin-fortune-from-us-entrepreneur-in-spain/)

In the Proposed Regulations, wallet companies would unnecessarily be required to collect and hold significant customer ID, including TINs and wallet addresses, therefore drawing a link between the two and ensuring another 'honeypot' for targeting by bad actors. Rather than ensure this data is concentrated in the *actual* brokers who effectuate relevant transactions and therefore require this data, the IRS is instead asking for it to be spread between multiple companies, with no discernible benefit for tax compliance benefits. To help ease the risks involved, the IRS should only require information collection and retention where it is necessary.

➔ **(4) The Proposed Regulations do not promote responsible innovation, representing an analog proposal for a digital age.**

Finally, the Proposed Regulations misinterpret the role that self-hosted wallets have in the wider digital asset ecosystem, seeking to impose financial-specific regulations, and may inadvertently impede the promising and innovative potential of self-hosted wallets.

To highlight the various uses of self-hosted wallets to contextualize their wider role, it should be noted that self-hosted wallets can also be used for non-financial instruments, which nonetheless hold value for the user. For example, they could include private credentials that hold a digital identity, which can be used in the way that a driver's license is used right now to prove somebody is eligible to fly at an airport. Many states are aware of the need to create digital IDs (DIDs) and have taken steps to *improve* how citizens can access their IDs online, although there is a clear need to go further and make these DIDs digitally native, through decentralization and credentialization. [32]

Furthermore, wallets reduce counterparty risk and promote consumer protection, which could be undercut if onerous reporting requirements discourage regulated entities from interacting with self-hosted wallet providers. As discussed, customers often hold their assets on custodial platforms - such as exchanges - where they are often held as 'balances' on an internal ledger rather than as a property right to a digital asset on the blockchain. In the event of an operational disruption or bankruptcy of that exchange or platform, there is a high risk that a customer would not have access to their assets. Self-hosted wallets represent a form of consumer protection, ensuring users can interact easily with exchanges but remain ultimately responsible for, and in control of, their digital assets.

---

[32] https://www.apple.com/newsroom/2021/09/apple-announces-first-states-to-adopt-drivers-licenses-and-state-ids-in-wallet/

The regulations would also undercut a solution that is key to economic empowerment and financial inclusion in the digital age. A 2023 study by Wakefield Research, in partnership with Block, Inc and based on surveys with over 6,600 people found that the 'majority of adults — 55% — have experienced things like credit card theft, physical cash theft, identity theft, or other negative financial- or privacy-related events' and that '78% have had negative experiences — needing to maintain a minimum account balance, paying a monthly fee, experiencing longer-than-expected transfer periods taking, or being surprised by a fee' when working inside the traditional finance and banking structures. [33] Self-hosted wallets, on the other hand, give power to everyday users to manage and control their assets in the way that they choose, without many of the risks listed above, giving them the security and accessibility they need.

At present, the Proposed Regulations would hinder American leadership and preclude involvement in technological innovation that is being undertaken in the global financial system. Fundamentally, wallets *enable* access to digital assets, but they *do not themselves hold or control* these assets. The Proposed Regulations risk inappropriately "pigeonholing" an ecosystem, and would lead to companies being unable to service the non-financial aspects of self-hosted wallets, instead focused on unnecessary and impossible compliance for transactions that the self-hosted wallet provider is neither party to nor has visibility on. We urge the IRS to consider a balanced approach that encourages responsible innovation and allows for the continued development of self-hosted wallet technologies.

*****

We greatly appreciate your consideration of our shared comments and are open, engaged, and ready to respond or discuss any further details with you at your convenience. We believe that self-hosted wallets have multiple, untapped benefits - financial and non-financial - and play a crucial role for everyday Americans as their digital lives continue to evolve with wider technological innovations. We look forward to hearing back from you, and to further the development of balanced regulations that continue to enable the innovations of self-hosted wallets.

Yours sincerely,

[33] https://block.xyz/inside/report-bitcoin-survey-2023

Amanda Anderson
Global Head of Public Policy
Block, Inc.
amandaanderson@block.xyz

Jai Massari
Cofounder & Chief Legal Officer
Lightspark Group, Inc.

Zachary Herbert
Cofounder & CEO
Foundation Devices, Inc.
zach@foundationdevices.com

Roy Sheinfeld
CEO
Breez Development LTD.

James Gernetzke
Chief Financial Officer
Exodus Movement, Inc.

William C. Hughes
Senior Counsel & Director
Consensys Software Inc.
william.hughes@consensys.io

Seth Hertlein
Vice-President, Global Head of Policy
Ledger.
seth.hertlein@ledger.com

Lawrence Zlatkin
Vice President, Tax
Coinbase Global, Inc.

Jonathan Jachym
Global Head of Policy & Government Relations
Kraken Digital Asset Exchange.

Jeff Rundlet
Head of Accounting Strategy
Cryptio.
jeff@cryptio.co

Pierre-Marie Padiou
CEO & Co-Founder
ACINQ.

Nick Neuman
CEO & Co-Founder
Casa, Inc.

Salman Banaei
Head of Policy
Uniswap Labs.