coinbase

To:

Australian Government
Attorney-General's Department
Via online submission

Date:

13 June 2024

Re: Reforming Australia's anti-money laundering and counter-terrorism financing regime (second stage consultation)

Coinbase Global, Inc. and its subsidiary Coinbase Australia Pty Ltd (together, **Coinbase**) welcome the opportunity to comment on the Attorney-General's second round of consultation papers relating to reforming Australia's Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) regime.

Our response focuses on the specific questions related to digital currency activities. We suggest some amendments to the expanded range of regulated digital currency-related services, as well as some practical considerations related to the implementation of Travel Rule (based on our experience in other jurisdictions). We respectfully push back against the implementation of international funds transfer reporting at this stage: we consider it to be an ineffective method to support the regulatory aim of assisting law enforcement, and note that it will be operationally extremely difficult to implement (especially given the other significant regulatory changes that will affect digital asset service providers in the near future).

We appreciate your thoughtful efforts to develop and modernise the Australian AML and CTF regime, and we look forward to continued engagement.

Sincerely,

Tom Duff Gordon
VP, International Policy
Coinbase Global, Inc.

John O'Loghlen
Country Manager
Coinbase Australia Pty Ltd

coinbase

Introduction

Coinbase is committed to the Australian market, and its local entity, Coinbase Australia Pty Ltd, is a current reporting entity registered with the Australian Transaction Reports and Analysis Centre (AUSTRAC).

As well as seeking to be the most trusted brand serving the Australian market with our products and services, we are also committed to being a trusted party in the development and regulation of Australia's blockchain and web3 sectors. We believe that a thoughtful approach to policy will play an important role in securing the continued and future vitality, competitiveness, and resilience of Australia's financial services and technology sectors. We have been an active contributor to the policy dialogue in Australia, and have most recently responded to the Attorney-General's first round consultation on *Modernising Australia's AML and CTF Regime* in June 2023, as well as the Treasury's consultation on *Regulating Digital Assets* in December 2023. We are honoured to contribute our thoughts and expertise to the Attorney-General's second round of consultation on *Reforming Australia's Anti-Money Laundering and Counter-Terrorism Financing Regime.*

Coinbase has always strived to be the most trusted company in the crypto-ecosystem - everywhere we operate. We built our business on that premise, with security and compliance at the core. We further believe that compliance is a cornerstone of a secure and thriving ecosystem and that public-private dialogue is crucial to ensuring users are safe and bad actors are identified.

While the Compliance team at Coinbase focuses on a number of distinct compliance disciplines, the largest group within the Compliance team is dedicated to financial crimes compliance (FCC), including AML, sanctions, and anti-bribery and corruption. Our FCC Program incorporates all of the components and controls customers expect from a traditional financial institution - from policies and procedures, to training, to customer due diligence. But the unique characteristics of digital assets - especially the public ledger of transactions within the blockchain - also provide innovative opportunities to identify bad actors and keep the ecosystem safe.

In addition to the tools we deploy, we recognised the need for global coordination on issues that transcend companies and borders - including Travel Rule compliance. We created an industry consortium, and eventually helped launch the Travel Rule Universal Solution Technology (TRUST) to move the entire industry forward. Today, TRUST includes 100 entities around the world, allowing them to comply with the Travel Rule while also protecting the privacy and security of their customers. We will address TRUST in further detail below in the substance of our submission response.

coinbase

In our submission from June 2023 in response to the Attorney-General's first consultation on reforms to Australia's AML and CTF regime, we described the unique attributes of blockchain-based solutions (such as blockchain analytics / "know-your-transaction" (KYT) tools like Coinbase Tracer) in fighting financial crime. We would like to draw the Attorney-General's attention to that submission again, in light of our responses below.

Note that we have not provided responses to every question in the five consultation papers but have focused our input on the specific questions related to digital currency activities.

Paper 4: Further information for digital currency exchange providers (DCEPs), remittance service providers and financial institutions

Expanding the range of regulated digital currency-related services

a. Do you consider that the current term and associated definition of 'digital currency' is appropriate? What alternative terms outside of 'digital asset' might be considered, and why?

We agree with the expansion of the definition from "[digital] currency" into "[digital] assets", and the intention to align terminology with other Australian Government developments.

We would further argue for alignment not just across government departments, but also globally. The Financial Action Task Force (FATF) uses the phrase "virtual assets" rather than "digital assets" and, given the global nature of blockchain technology, we would advocate for consistency with international bodies, not just bodies within Australia.

b. How should the scope of NFTs subject to AML/CTF regulation be clarified?

We note that one of the rationales for amending the definition of "digital currency" is to enable non-fungible tokens (NFTs) to come within the regulatory standards applied to forms of digital "currency". We also note the FATF recommendation that generally NFTs should not be subject to the global FATF standards where they are in practice used only as collectibles rather than a means of transfer of value - and instead, regulators should look beyond just marketing terms to determine whether something practically functions as a means of payment or an investment instrument.

Whilst we appreciate the principle that NFTs which are collectibles should not be subject to the FATF standards, we note that classification as "collectible" may be difficult to ascertain in practice. Additionally, an NFT may launch as a collectible and then later be used as a means of payment, sometimes contrary to the intentions of the issuer; in such instances, it would be difficult for the issuer to ascertain exactly when their regulatory obligations would start (how widely does an asset need to be used as a means of payment or an investment instrument before it is subject to regulation? How does an issuer know exactly how their asset is being used in practice?).

In the interests of regulatory certainty, we would request that, if the regime is to cover any type of NFT, then there should be very clear guidelines as to how to ascertain when a token has passed from "collectible" into "means of payment or investment instrument".

c. Are there any services that may be covered by the term 'making arrangements for the exchange…' that should not be regulated for AML/CTF purposes?

The phrase "making arrangements for the exchange" is wide and arguably could include the provision of software that allows users to self-custody their assets. But the provision of mere software should not be caught by Item 50A of Table 1 in section 6 of the Act, or in any other manner within the proposed amendments. Excluding self-hosted wallets and the software enabling such self-hosted arrangements from the AML/CTF regulatory remit would be consistent with the approach seemingly taken by Treasury in its October 2023 *Regulating Digital Asset Platforms* Consultation Paper (see p.12), as well as the approach taken in other comparable jurisdictions[1].

Assuming that "making arrangements for the exchange…" is not intended to capture software enabling self-hosting arrangements, this should be clarified through redrafting or secondary guidance.

d. Is the proposed language around custody of digital assets or private keys clear?

We broadly agree with the high level wording of "Proposed designated service 3" in the consultation. However, the explanatory notes as to what constitutes "custodial services" state "custodial services could include persons who have custody of: … one of multiple private keys in a multi-signature arrangement, or smart contracts to which they are not a

[1] HM Treasury, *Future financial services regulatory regime for crypto assets: Response to the consultation and call for evidence*, p.59, 8.13 'Self-hosted wallets' (October 2023) https://assets.publishing.service.gov.uk/media/653bd1a180884d0013f71cca/Future_financial_services_regulatory_regime_for_cryptoassets_RESPONSE.pdf

party" without clear indication of how control should be considered in making the determination.

With regard to multi-signature arrangements, any definition of "custody" should only extend to circumstances where a wallet provider exercises total independent control over the value held in the wallet – i.e., the provider holds the wallet's private keys, or otherwise has the means to *unilaterally* withdraw funds from the wallet - and avoid capturing standard wallet provisions, or other non-custodial multi-signature arrangements, such as those primarily intended to enable access recovery if the user loses their primary key shard. This would help ensure that the definition of "custody" encompasses providers who act as intermediaries in payment flows and, therefore, should be subject to the applicable suite of AML and know your customer (KYC) obligations. By contrast, where a provider does not hold the private key(s) sufficient to unilaterally withdraw funds from a wallet, they are neither a custodian nor an intermediary, but are acting as a software provider that is not engaging in money transmission. The requirement to have independent control over the value held in the wallet is an approach which has been taken in other jurisdictions[2].

With regard to smart contracts, this wording is currently wide and ambiguous. Not all smart contracts relate to financial services or the exchange of value (e.g. use of smart contracts for sharing of data between different parties, or use of smart contracts in digital identity services). Too wide a definition of smart contracts would have the effect of bringing all these types of smart contracts, which themselves do not pose any AML/CTF risk, within the remit of the AML/CTF regime unnecessarily.

Additionally, it is not clear what is meant by "hav[ing] custody of… smart contracts to which they are not a party." For instance, does this only refer to persons who have custody over assets held on a smart contract (i.e., those who have "total independent control" over the assets, as described above)? Or would it more broadly extend to contract providers who may not custody assets on a smart contract but nevertheless have some measure of control over the smart contract itself – for instance, the ability to *unilaterally modify* a smart contract? If so, then this definition would, it seems, catch the very networks on which smart contracts are built, because it is the network itself which automatically executes the contract in question.

Given the decentralised nature of many blockchains or Layer 2 (L2) networks, imposing AML/CTF obligations on them through catching them within the definition of providing "custodial services" would be extremely difficult in practice. Further, where the smart

[2] E.g. FinCEN Guidance FIN-2019-G001, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies,* section 4.2 https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf

contract provider lacks total independent control over assets held on the contract, we would again note that they would operate more as mere software providers, not intermediaries within the payment flows that may occur via the contract.

Thus, the explanatory notes defining what constitutes "custodial services" should be collapsed into a single definition of instances where a provider has total and independent control over the asset in question (this is the approach taken in the FinCEN Guidance referenced above).

Streamlining value transfer service regulation

f. Are there any services currently provided by financial institutions that fall outside the definition of 'electronic funds transfer instruction', but would be captured by the 'value transfer' concept?

Whilst this is not a service currently provided by financial institutions, we would like to clarify here whether the provider of a smart contract may or may not be caught by this new concept of "value transfer". For example, could the provider of a smart contract be caught as an "ordering institution" where it initiates a smart contract on the instruction of its customer, even if the actual value transfer is contingent on other actions / events, and if the value is then transferred by the smart contract (i.e. network), rather than the provider itself?

We would suggest that the proposed new value transfer definition be amended such that it is clear that any "ordering institution" must themselves actually initiate a transfer of value, rather than initiate anything else which might subsequently result in a transfer of value.

g. Is the terminology of ordering, intermediary and beneficiary institutions clear for businesses working in the remittance and digital asset service provider sectors?

For businesses working in the digital asset service provider (DASP) sector, it is unlikely that an "intermediary institution" will exist for most (if not all) transfers. Additionally, in many instances - in particular transfers to and from self-hosted wallets - it is likely that there will only be *either* an ordering, *or* a beneficiary institution (or in some cases, neither). We assume that where a particular institution is not relevant to a transaction, that will simply mean that there is no "designated service" provided in respect of that side of the transaction.

coinbase

Updates to the Travel Rule

Before responding to the individual consultation questions, we would first like to note our appreciation in the proposals that transfers from DASPs to self-hosted wallets (and vice versa) will attract only limited Travel Rule obligations. However, we would like to clarify what exact data points will be required for "Travel Rule information", and in particular whether counterparty information is expected to be collected. Where the transfer is to/from a self-hosted wallet, the only way to obtain counterparty information would be for the DASP to ask their own customer. However, customers may not be able to obtain this information accurately from their counterparty, or, for entirely legitimate reasons, may have no direct relationship with the counterparty (such as where the counterparty is a merchant or a smart contract).

Further, it would be impossible to verify any information that is collected; the DASP collecting this data will have no contractual terms of service with the counterparty, and will thus have no way of compelling the counterparty to verify the accuracy of the data. In such cases, bad actors could simply provide false information about their counterparties, leaving DASPs with inaccurate data in their systems. Bad data coming into compliance systems will lead to bad data going out in the form of inaccurate suspicious matter report (SMR) filings and data sharing (pursuant to Section 49 of the AML/CTF Act or other law enforcement request for further information) - which would be a detrimental outcome for regulators and law enforcement.

Additionally, we would like to confirm the proposal around DASPs collecting and/or verifying payee information for transfers to another DASP (rather than self-hosted wallets). Given our concerns regarding the collection of non-customer information (which we articulated in our response in June 2023 to the Attorney-General's first round consultation on AML and CTF regime reform[3], as well as above in the context of transfers to self-hosted wallets), we would be grateful if it could be specifically confirmed in secondary guidance whether collection and transmission by an ordering institution of *payee* information (or, for that matter, the collection and transmission by a beneficiary institution of *payor* information) will be required for DASP<>DASP transfers.

[3] *Modernising Australia's AML and CTF Regime*
https://assets.ctfassets.net/c5bd0wqjc7v0/5oqawnWTfFF97F4eCFgJJW/7aa32c17a7862a971eaea010c0eba645/Coinbase_response_to_Australia_AML_CTF_Consultation_-_June_2023.pdf

coinbase

i. **What flexibility should be permitted to address the sunrise issue or where a financial institution or digital asset service provider has doubts about an overseas counterparty's implementation of adequate data security and privacy protections? What risk mitigation measures should be required?**

In regard to the "sunrise issue", Coinbase appreciates the Attorney-General's acceptance of a risk-based approach to determining whether to make value available to the payee for incoming transfers lacking travel rule information. We would argue that the same risk-based approach to completing a transfer should be allowed in cases where an ordering DASP has doubts about an overseas beneficiary's implementation of adequate data security and privacy protections.

In both cases, legislation and AUSTRAC guidance should not be overly prescriptive as to what must be considered in a "risk-based approach" and what risk mitigation measures should be required. For example, it should not be a requirement that the country of origin of a transfer *must* be considered in all cases, given the challenges of knowing for certain the jurisdiction from which a digital asset transfer has originated, or to which a digital asset transfer is going. Where a DASP is not able to determine with reasonable accuracy the relevant counterparty jurisdiction, it would not be able to factor in country risk to its overall risk assessment for that particular transfer. In all cases, DASPs should be free to determine their own risk-based approach, given the circumstances of each transaction. However, basic risk mitigation measures that could be suggested in guidance would be:

- Use of blockchain analytics services to screen incoming and outgoing transactions and assign wallet addresses with a risk rating based on previous activity;
- Sanctions interdictions tools or blocklists for sanctions-related addresses; and
- Use of transaction monitoring scenarios, based on transaction volume and other indicators, to trigger additional customer due diligence.

DASPs should be allowed the flexibility of taking "reasonable measures" to exchange Travel Rule information with a counterparty, rather than any requirement for 100% compliance being enforced. That is to say, where a DASP has taken reasonable measures to make Travel Rule information available to a beneficiary DASP (or obtain Travel Rule information from an ordering DASP), those steps should be sufficient to allow the value transfer to be made available. That is to say, there should be no blocking of transactions where Travel Rule information cannot be exchanged despite a DASP's reasonable efforts to do so. Blocking transactions merely pushes customers to use self-hosted wallets, or offshore DASPs - this in turn moves transactions further away from law enforcement's ability to follow funds by requesting information from centralised and onshore DASPs.

coinbase

k. Are there challenges for financial institutions reporting cross-border transfers of digital assets, including stablecoins, on behalf of customers?

We would be grateful if the Attorney-General could clarify the wording of this question (the fact that it refers to the "reporting" of cross-border transfers), given that the consultation itself states "The travel rule is a record-keeping and data transmission requirement, not a reporting requirement" (see page 12 of Consultation Paper 4). We have assumed for the purposes of this response that this question refers to general challenges for Travel Rule compliance where transfers are cross-border.

As acknowledged in the consultation, a key challenge for cross-border transfers is the sunrise issue, as well as different standards for wider regulatory obligations applying to DASPs (e.g., differing data protection and privacy standards). In fact, some DASPs purposefully choose to operate out of jurisdictions with lower general compliance obligations; it is important that the implementation of Travel Rule in Australia is not overly prescriptive or strict, such that the level of customer friction results in customers being pushed to use these offshore operators.

Two key challenges (applying to all transfers of digital assets, not just cross-border ones) are the practical questions of (i) how to identify the counterparty DASP, and (ii) how to transfer Travel Rule information, even once a counterparty has been identified. The industry has successfully responded to these problems; as mentioned above, Coinbase has worked alongside a large group of DASPs over the last few years to pioneer the development of TRUST - a Travel Rule solution that allows DASPs to accurately identify their counterparties and securely exchange required data.[4] We have invested significant legal, compliance, engineering, and other resources to build the TRUST solution, which DASPs around the world are already using to exchange information required under the Travel Rule.

TRUST's rapid growth since its launch in 2022 is a testament to the industry's commitment to solving complex compliance challenges. TRUST today includes 100 entities across 16 different jurisdictions and continues to expand globally, as it is designed with the flexibility to adapt to different regulatory requirements across jurisdictions. All DASPs who join TRUST undergo comprehensive due diligence to help ensure that their security protocols are equipped to prevent unapproved access to sensitive customer data shared by TRUST participants (thus addressing the concerns noted above around differing data protection and privacy standards). Further, TRUST was designed so that no customer PII is stored on a centralised database, but is instead only shared directly between counterparty DASPs via encrypted, peer-to-peer channels, reducing the risk of hacking or improper access. These

[4] See https://www.coinbase.com/travelrule, describing the TRUST solution and listing DASPs who have joined the TRUST coalition

and other features have been critical to TRUST's growth to become the world's leading Travel Rule solution.

Importantly, Coinbase engaged closely and repeatedly with regulators around the world while designing and launching TRUST. This approach of collaboration and encouraging industry innovation has proven very effective, as compared to issuing unilateral rules that dictate how to solve certain concerns, without industry input on the actual risk, unintended consequences, and alternatives available. We encourage the Attorney-General to follow this approach in seeking industry input to collaboratively understand other risks and develop effective solutions; we would be delighted to provide the Attorney-General with more details relating to TRUST.

Reforms to IFTI reports

n. What should be the 'trigger' for reporting IFTIs? At what point is a reporting entity reasonably certain that the value transfer message will not be cancelled or refused and the value transferred?

For transfers of fiat funds through many types of existing systems, such as SWIFT, the actual transmission of value occurs at a readily identifiable point in time and therefore it is easier to identify the time at which IFTI reporting should be triggered.

By contrast, in the context of digital asset transfers, this can be more ambiguous for several reasons. A digital asset transfer that occurs on a permissionless, decentralised blockchain, such as the Bitcoin or Ethereum blockchain, must be validated by a sufficient number of network participants before it is considered final. The number of confirmations required to consider a transfer final, and the pace of such confirmations, affect how much time is required before the transfer of value is considered complete. These, in turn, depend on the specific kind of digital asset being transferred and the finality standards maintained by the DASP parties to the transfer, each of which may have their own standards for the number of confirmations required before crediting the receiving account. Therefore, the point at which the transfer of value actually occurs (i.e., when the receiving DASP credits the funds) and, accordingly, when the IFTI report should be made, may be unclear and will vary depending on the DASP in question.

As is further explained in the response to question (p) below, Coinbase would generally argue against the implementation of IFTI reporting for DASPs at this stage, and in any event would suggest a number of amendments to the requirements (such as a threshold for reporting). However, if IFTI reporting is indeed implemented for DASPs as proposed, we broadly agree with the proposal that a reporting entity is reasonably certain that the value transfer message will not be cancelled or refused and the value transferred when: (a), in

the case of incoming transfers, the transferred value is made available to the payee as a result of the individual DASP receiving sufficient confirmations to meet its own finality standards, and when (b), in the case of outgoing transfers, the transaction is initiated on-chain.

o. What information should be required to be reported in a unified IFTI reporting template, covering both IFTI-Es and IFTI-DRAs?

Please refer to our answer at question (p) below regarding data privacy concerns and in particular our suggested changes to the data fields required.

p. Are there challenges with digital asset service providers reporting IFTIs to AUSTRAC as proposed?

Coinbase has significant concerns with the application of IFTI reporting to DASPs. Above all, identification of "international" digital asset transfers is almost impossible given the fundamental nature of blockchain technology, and reporting would be operationally very difficult for DASPs, given the lack of automated reporting mechanisms. We also have concerns from a data privacy perspective, and overall we consider that IFTI reporting is an ineffective and disproportionately burdensome way of furthering the ultimate goal of assisting law enforcement. We argue that IFTI reporting be postponed at least until after the Travel Rule has been implemented and, even then, be subject to threshold limitations to reduce the operational impact on DASPs (especially given significant other incoming regulatory requirements, including wholesale licensing changes and the Travel Rule, which will already be very impactful for DASPs).

Operational challenges and concerns

As has been noted in the context of Travel Rule obligations above, in respect of digital asset transfers, it is not generally possible to ascertain whether the transfer in question is cross-border, as the location of the counterparty wallet cannot always be determined; a permissionless blockchain does not indicate where a sending or receiving wallet address is based. Where a DASP is providing custodial services, there is also the question of situations where a wallet may be hosted offshore, but the beneficiary of that wallet is based in Australia (e.g. the end customer is a user of a global DASP, whose omnibus wallets are all hosted outside of Australia). In such instances, it is not clear if an IFTI report would be required because the wallet itself is based overseas, or whether a report is *not* required because the end user who benefits from the value transfer is based in Australia.

In any event, given the inherently borderless nature of digital assets transactions, the number of transactions likely to be subject to IFTI reporting would be extremely large. We

have reviewed transaction data for Coinbase Australia from May 2024 to estimate reporting numbers. As described above, we cannot know with certainty the destination or origin of on-chain transactions; however, extrapolating from off-chain sends, we estimate that our users completed over 57,000 international transactions on-chain in the month of May 2024. This would suggest that IFTI reporting may result in nearly 700,000 reports being filed by Coinbase Australia to AUSTRAC every year. This scale of reporting would be operationally extremely burdensome on DASPs, especially given the current absence of automated reporting mechanisms; it would also result in a very large number of reports being received by AUSTRAC.

It may be possible in some cases for a DASP to have its customer answer questions about the destination or origin of funds, but such information will not always be reliable or available (as detailed above in the context of the Travel Rule). This uncertainty will create inaccuracy of reporting and undermine the primary purpose of the reporting, which is to aid law enforcement.

Beyond the challenge of knowing the location of an ordering or beneficiary wallet, there is also the challenge of how to submit IFTI reports at scale without requiring significant manual effort. We understand that financial institutions to which IFTI reporting obligations currently apply are able to complete and submit reports to AUSTRAC automatically through use of SWIFT messages in MT or ISO20022 formats. Such an automated system does not exist for DASPs, which would result in reporting either being through manual entry, or the uploading of a spreadsheet/ other file format. Both approaches would involve significant operational overheads, as well as data risk.

Data risk

We note that the department proposes to abolish the distinction between IFTI-Es and IFTI-DRAs, and merge the two report types into a single harmonised IFTI report, the contents of which are being considered. It is therefore not clear exactly which data fields would be required for IFTI reports to be filed by DASPs - but we have assumed that the IFTI-DRA for designated remittance arrangement is most analogous to a transfer of value through digital assets. As such, the IFTI report for a digital asset transfer would need to include:

- Details of the ordering customer and beneficiary customer including their full legal name - not initials or abbreviations,
- Customer Identification details such as ID type and ID number,
- Customer address details (i.e. customer's physical address), and
- Details of the transfer instruction, such as transfer date, type of currency, the direction of the transfer and transaction reference number, if applicable

First, and as mentioned above in relation to implementation of the Travel Rule, ordering DASPs do not currently hold details on the beneficiary to a transaction, and nor do beneficiary DASPs hold details on the ordering customer. As such, until Travel Rule requirements are implemented (and depending on exactly what is implemented), DASPs will not even be in a position to provide all the above data for IFTI reporting. Additionally, they may not have a legal basis under privacy laws to do so - for example, DASPs who do not currently hold this information may be required to collect additional personal information in order to comply with the reporting requirements. This means that DASPs would need to make operational changes to their global data collection practices (e.g. identifying legal bases for collecting and sharing these new categories of personal information), which would have privacy implications for individuals located both inside and outside of Australia.

Additionally, the above includes some of the most high-risk types of personal information that DASPs collect on their customers, and the transmission of such information would create a honeypot for bad actors interested in targeting customers of DASPs. We are concerned about the increased risk of a data breach where large amounts of personal information are being collated and transferred. In particular, if this type of information is compromised, this would have a high risk of causing serious harm to affected customers, as it may give rise to identity theft and financial loss through fraud.

Ineffective tool for combatting digital asset financial crime

We do not consider that there is an inherent risk associated with a transfer of digital assets merely because that transfer occurs cross-border, and as such there is no clear basis for transmitting such high-risk personal information at scale. It is hard to see how mass reporting of cross-border transactions would be incrementally beneficial to law enforcement who, when it comes to transactions on the blockchain, have tools available to them that are not available in the context of traditional financial services. Blockchains collect all transactions and record them on a common, public ledger, which means that DASPs, along with regulators and law enforcement, can analyse transactions carried out on that blockchain.

In contrast, a traditional financial institution is largely limited to using private, opaque ledgers that are only available to that specific institution. This creates significant risk of blind spots for traditional financial institutions as well as law enforcement because it is difficult - if not impossible - for them to fully monitor all transactions. In such an environment of private, opaque ledgers, it is clear that large-scale IFTI reporting is beneficial to law enforcement who would otherwise have no visibility into transactions that occur. This is not the case for digital asset transfers that are recorded on the blockchain. Public ledgers mean DASPs and law enforcement can conduct sophisticated analyses to determine the risk of a specific transaction or asset. An entire industry of blockchain

analytics firms have developed in recent years to assist both DASPs and law enforcement in utilising the abundant data available on public blockchains, thus reducing the need for concepts like IFTI reporting. Real-time blockchain analysis is also quicker and more efficient than relying on IFTI reporting from DASPs.

Additionally, IFTI reports provide information on a transaction and a user at a snapshot in time. The reports are of limited use without the context of the entire customer relationship and the previous activity undertaken by the user in question. By contrast, the DASPs hold details of the historic customer relationship and are able to contextualise the transaction to determine whether it is of concern. A suspicious matter report, filed by a DASP after an alert from its own transaction monitoring program and after consideration of the full customer relationship history, will always be more beneficial than a one-off IFTI report.

Overall, Coinbase would argue that the regulatory aim of assisting law enforcement with combatting and disrupting financial crime would be better served (and be more proportionate in terms of operational burden for DASPs) by a combination of:

- DASPs and law enforcement bolstering their transaction monitoring programs and use of blockchain analytics, as well as DASPs ensuring that their SMR processes are as accurate and comprehensive as possible; and
- Making sure Travel Rule implementation for DASPs is a success, such that DASPs hold relevant transactional data should they be issued with a section 49 notice, or other law enforcement request for further information.

It is important to note that Compliance and private sector assistance with law enforcement can take two forms. The first is mandatory reporting (such as is proposed by the consultation); the second is the building of strong bilateral relationships between public and private organisations, in the general interest of protecting customers and the wider ecosystem. Coinbase believes that public-private dialogue is crucial to ensuring users are safe and bad actors are identified. Coinbase has partnered with the Australian Police Force as part of the Joint Policing Cybercrime Coordination Centre (JPC3) and shared ways by which Coinbase works with law enforcement around the world. This cooperation has also extended to engagement with the JPC3 representative teams of the “Big 4” banks and is an example of how innovative companies can and should work together with the public sector on issues such as security and compliance, and of our commitment to do so in Australia. The implementation of mandatory reporting is not the only way to allow for private corporations to support law enforcement efforts.

Timing of implementation of IFTI reporting

As mentioned above, there are significant regulatory uplifts pending for DASPs which will require substantial operational change (most significantly, the Travel Rule and incoming

licensure changes currently being considered by Treasury). Additionally, we consider that the Travel Rule for digital assets may largely accomplish the same goals as IFTI reporting.

As such, we suggest waiting to implement IFTI reporting until after the Travel Rule has been fully implemented by DASPs. At such time, law enforcement will have had the benefit of information sharing and record keeping required by the Travel Rule, so will better understand whether IFTI reporting would be incrementally beneficial. Additionally, solutions and networks for the sharing of digital asset transaction data will have matured and may better enable automated reporting. Crucially, postponing the implementation of IFTI reporting would allow for small businesses to spread the operational impact of the significant regulatory change to which they will be subject in the coming months.

Proposed changes to scope of reporting

For the above reasons, Coinbase would argue against the implementation of IFTI reporting for DASPs, or at least for the delay of implementation. In any event, should the Attorney-General proceed with requiring funds transfer reporting, we propose the following amendments to the scope:

- **A threshold for reporting** - we would suggest an A$10,000 threshold for reporting in respect of digital asset transactions. This would be in line with the threshold at which travellers need to report the cash they are carrying into or out of Australia, and be in line with approaches taken for digital asset transaction reporting in other comparable jurisdictions[5]. It would also have the effect of targeting reporting to the highest value transactions (which represent higher financial crime risk), as well as managing some of the operational concerns noted above. Above, we noted that Coinbase Australia estimates over 57,000 international transactions were completed by its users in May 2024; excluding transactions of <A$10,000 in value would reduce the reportable number of transactions to less than 700 for May, which is a significantly more manageable number.
- **Removing the requirement that the funds transfer be "international"** - as described above, determining the geographical origin or destination of digital assets transfers is challenging. Removing the need for reporting to hinge on "international" transfers would significantly simplify the operational implementation of transaction reporting for DASPs. When combined with the monetary threshold suggested above, this would be in line with other jurisdictions that require reporting based solely on a

[5] E.g., Large Virtual Currency Transaction Reporting in Canada (https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/lvctr/lvctr-eng) or "unusual transaction" reporting in the Netherlands (https://www.fiu-nederland.nl/en/reporting_group/exchange-between-virtual-currencies-and-fiduciary-currencies/) (noting that in the Netherlands, the thresholds are €15,000 for all transactions, or €10,000 for exchanges between digital assets and fiat currency). In both countries, reporting applies regardless of the geographical destination or origin of funds.

monetary threshold, rather than geographic origin or destination (see footnote 5). Of course, expanding the scope of reporting to cover all transactions (not just international ones) would increase reporting numbers, but from our transaction data, this would not be problematic so long as the A$10,000 threshold were implemented - in May 2024 data, 1,192 transactions would have been in scope of reporting.

- **Reduced data fields** - given one of our key concerns relates to data security given the sensitivity of the data fields contained within IFTI-DRA reports, we suggest that the reports for digital asset transactions instead contain a reduced number of fields (e.g. just the name of the DASP's customer, as well as transaction information). Where such information matches with a line of enquiry being pursued by law enforcement, then DASPs would be able to provide additional information on production of a request for further information. In any event, if the DASP does not already hold the relevant information it should not be required to collect additional data fields in order to satisfy the reporting requirements.

We would be very happy to discuss the operational challenges described above, as well as the proposed changes to scope. We look forward to continued partnership in fighting financial crime in Australia.