coinbase

To:

Australian Government
Attorney-General's Department
Via online submission

Date:

16 June 2023

Re: Modernising Australia's anti-money laundering and counter-terrorism financing regime

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

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 strives to be the most trusted platform here. We are proud that Coinbase has established a local entity (Coinbase Australia Pty Ltd) and obtained registration and enrolment as a digital currency exchange with the Australian Transaction Reports and Analysis Centre. Beyond our endeavours to serve the Australian market with our products and services, we are also committed to responsible stewardship as Australia develops its web3 sector. As such, we serve as a board member of Blockchain Australia and have partnered with many web3 ecosystem players in Australia, like Zepto and CryptoTaxCalculator; we have also worked with multiple university blockchain departments and web3 innovation centres. 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. That is why we have been an active contributor to the policy dialogue with the Treasury and others, including our recent submission to the Treasury's token mapping consultation, and why we are honoured to contribute our thoughts and expertise to the Attorney-General's consultation on *Modernising Australia's Anti-Money Laundering and Counter-Terrorism Financing Regime.*

Coinbase has always strived to be the most trusted company in crypto—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. Coinbase recently 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.

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 crypto—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 more than 80 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 content of our submission response.

In our response today, we will be discussing the unique attributes of blockchain-based solutions in fighting financial crime before addressing the consultation's queries with direct pertinence to digital assets and crypto. We applaud the Australian Attorney-General's efforts to modernise the AML/CTF regime, and hope we can contribute unique, leading insights into the constructive role crypto firms may play to help reach this goal.

Blockchain-Based Compliance Solutions

Companies like Coinbase have devoted enormous resources to developing effective compliance programs. This includes traditional controls like collecting KYC information, monitoring on-platform transactions, and filing Suspicious Matter Reports ("SMRs"), but more critically, deploying innovative technologies that leverage the public and transparent nature of the blockchain, which is not constrained by private ledgers.

Blockchains collect all transactions and record them on a common, public ledger. This means that Virtual Asset Service Providers ("VASPs"),[1] along with regulators and law enforcement, can analyse transactions carried out on that blockchain—whether or not they took place on the VASP's own platform.[2] 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 because it is difficult—if not impossible—for them to fully monitor transactions that happen

[1] This Comment adopts the definition of "VASP" put forward by the Financial Action Task Force ("FATF"): "any natural or legal person who . . . as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: (i) Exchange between virtual assets and fiat currencies; (ii) Exchange between one or more forms of virtual assets; (iii) Transfer of virtual assets; and (iv) Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; (v) Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset." FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* ¶ 44 (Oct. 2021), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf ("FATF October 2021 Guidance").

[2] See Ari Redbord, et al., *Home Alone? Never, with Transaction Monitoring*, (Sept. 22, 2022), https://www.acamstoday.org/home-alone-never-with-transaction-monitoring/ (emphasising how "the blockchain allows for unprecedented visibility on financial flows."); Michael Morell, et al., An Analysis of Bitcoin's Use in Illicit Finance 5 (Apr. 6, 2021), https://cryptoforinnovation.org/wp-content/uploads/2022/07/An-Analysis-of-Bitcoins-Use-in-Illicit-Finance-By-Michael-Morell.pdf ("A currently serving official at the [Commodity Futures Trading Commission] added that it 'is easier for law enforcement to trace illicit activity using Bitcoin than it is to trace cross-border illegal activity using traditional banking transactions, and far easier than cash transactions.'").

away from their individual platforms. For example, if a bank's client wants to deposit funds into an account, the bank must rely on information provided by the customer about the source of those funds. Crypto fixes this problem by giving VASPs unprecedented access to the full scope of transactional records.[3]

Public ledgers mean VASPs can conduct sophisticated analyses to determine the risk of a specific transaction or asset—using tools and methods broadly referred to across the crypto ecosystem as know-your-transaction ("KYT"). An entire industry of blockchain analytics firms have developed in recent years to assist both VASPs and law enforcement in utilising the abundant data available on public blockchains.[4]

KYT is groundbreaking for compliance because it is:

- **Immediate** - because the information is available on the blockchain;
- **Independent** - it does not have to come from the customer and cannot be tampered with[5]; and
- **Dynamic** - the risk associated with a customer or transaction can be continually reevaluated based on new blockchain data.

VASPs can combine KYT with traditional compliance tools to enhance their risk ratings of customers associated with those transactions. Whereas KYT is immediate, independent, and dynamic, traditional "Know Your Client" ("KYC") information is the opposite. It is based on financial institutions collecting static data points about a customer at the time of account opening, such as identification documents, account statements, corporate records—and typically only occasionally refreshing those data points.

VASPs like Coinbase incorporate KYT into many key areas of compliance programs, including transaction monitoring, customer risk ratings, and sanctions controls:

1. **Transaction Monitoring** - KYT tools (such as Coinbase Tracer) can be directly incorporated into transaction monitoring tools so that a VASP can be alerted when a

[3] See Jai Ramaswamy, *How I Learned to Stop Worrying and Love Unhosted Wallets: Former DOJ AML Chief Considers the Unintended Consequences of Unhosted Wallet Restrictions and the Regulatory Benefits of Cryptocurrency Adoption*, (Nov. 18, 2020).
[4] See FATF October 2021 Guidance ¶ 234 (noting that "[b]lockchain analytics are … widely used by VASPs … to monitor their own exposure to risk.").
[5] See Robert Werner, et al., *Blockchain Analysis Tool of Cryptocurrency, ICBCT '20: Proceedings of the 2020 The 2nd International Conference on Blockchain Technology 80* (Mar. 2020), https://dl.acm.org/doi/pdf/10.1145/3390566.3391671 ("The blockchain … is an immutable ledger, which is stored on a large network of servers worldwide in a decentralised manner. On this ledger, all transactions are stored permanently, transparently and can be accessed by anyone.").

customer engages in risky transactions, both on and off its platform—which includes transactions with both hosted and self-hosted wallets.[6]

2. **Risk Ratings** - VASPs can dynamically incorporate KYT into a customer's risk rating. While initial risk ratings based on KYC information are static because the information is collected at the time of account opening, KYT data (which leverages the blockchain) can be dynamically added to a customer's risk rating based on a customer's ongoing activity. If the rating rises to a certain level, VASPs can take further action, such as conducting enhanced diligence reviews, closing the account, or filing an SMR.

3. **Sanctions Controls** - KYT also creates an enhanced approach to sanctions compliance in which VASPs directly screen for crypto addresses identified by the U.S. Office of Foreign Assets Control ("OFAC") (or other governmental bodies that specifically sanction crypto addresses) and can then proactively build out larger networks of high-risk addresses (e.g., those addresses that interact directly with sanctioned crypto addresses). Before the advent of crypto, OFAC was limited to putting static, traditional identifiers—such as names and addresses—on its Specially Designated Nationals List. But with blockchain technology, sanctions compliance can now be based on transactional data, not just personal identifying information ("PII"). VASPs can take ground-truth addresses provided by OFAC to build out and identify much larger networks of high-risk counterparties using blockchain heuristics; that is to say, from a relatively small number of blockchain addresses identified by OFAC, VASPs can build out large networks of addresses that they do not allow customers to transact with. And they can do this by leveraging immutable transactional data on the blockchain that is unrestricted by private ledgers and can tell them about common ownership.

In our view, modernising AML/CTF means embracing modern tools that are groundbreaking in securing the safety and integrity of the financial system. We hope that the Attorney-General will find this brief overview on the benefits of blockchain technology for AML/CTF compliance a helpful background as we share further insights throughout our response below.

---

[6] *See, e.g.*, Chainalysis, *How Chainalysis Helps Compliance Teams Address Sanctions Red Flags* (Mar. 8, 2022), https://blog.chainalysis.com/reports/fincen-russia-sanctions-red-flags-chainalysis/ (describing how blockchain analytics tools can be customised, allowing compliance teams to "assign unique transaction thresholds for alerts to be triggered for different counterparty categories based on their own risk strategy.").

coinbase

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

Part 1: Simplifying and modernising the regime

Regulation of digital currency exchanges

14. What are the benefits and challenges of expanding the AML/CTF obligations to a broader range of digital currency-related services?

We are generally supportive of expanding the AML/CTF obligations to the broader range of digital currency services detailed in the consultation; as more Australians hold digital currencies, there will be less need for exchanges in and out of fiat, and in such cases, those transfers would fall outside the current scope of the AML/CTF regime. Additionally, we note that illicit activity, though representing an extremely small percentage of the total number of digital currency transactions[7], can be solely undertaken through crypto to crypto ("C2C") transactions, without the need for a nexus with the fiat world.

We appreciate the assurance that any expansion of the AML/CTF regime to cover a broader range of digital currency-related services would be aligned with any future reforms of the overall crypto asset services sector by Treasury, to minimise duplication where possible.

We note that, should AML/CTF obligations be expanded to cover a broader range of digital currency services, it will be vital to ensure that digital asset businesses are still able to make their own risk assessments. That is to say, the expansion of AML/CTF obligations should not apply any "one size fits all" approach to all digital currency service providers regardless of business model. For example, service providers who engage solely in the business of long-term custody of digital currency for solely Australian clients, where transfers in and out of custody are infrequent, may pose a lower AML/CTF risk than other types of business. Digital currency service providers should in all cases be left to identify, assess, and measure risks, and apply controls that are most appropriate for their business model.

[7] Chainalysis, *The 2022 Crypto Crime Report*, 4 (Feb. 2022) ("Transactions involving illicit addresses represented just 0.15% of cryptocurrency transaction volume in 2021 despite the raw value of illicit transaction volume reaching its highest level ever.").

coinbase

15. How can definitions under the Act be amended to integrate digital currency activity in payment-related obligations, such as activities associated with credit, debit and stored value cards and general transfers?

Definitions under the Act may be amended to integrate digital currency activity in payment-related obligations by expanding what is currently captured. For example, currently:

- the definition of 'stored valued cards' does not include things that give access to digital currency. This definition could be modified to do so by deleting (e)(iii) of the definition or a declaration being made in the AML/CTF Rules under (c) that things giving access to digital currency are captured;
- the remittance designated services and corresponding definition of 'designated remittance arrangement' is connected to the movement of money and property, which does not capture digital currency. These services and definition could be expanded to include the transfer of digital currency; and
- there is no designated service capturing the exchange of one digital currency for another, only fiat on and off ramps (see item 50A in Table 1 of section 6 of the Act). This definition could be expanded to include both activities. For example, "*exchanging digital currency for money or another digital currency and vice versa, where the exchange is provided in the course of carrying on a digital currency exchange business*".

However, this approach may present complications with respect to tracking how such definitions are used through the Act and Rules and creates difficulty for future developments. Coinbase submits that an alternative approach would be to consider inserting a new Table in section 6 of the Act to specifically cover digital currency related services.

Digital currency is a rapidly developing technology and it is likely that there will be new services in future that are not currently contemplated. Having a specific table for digital currency related services would provide an easier framework for future reform rather than reworking existing definitions under the Act. This would also allow AML/CTF reform to progress alongside other digital currency related reform (such as token mapping and licensing) without being hindered (that is to say the Attorney-General consultation may continue on with possible new designated services without needing to wait for the outcome of other reviews that may affect how Table 1 designated services are interpreted in the context of digital currency).

coinbase

Modernising the travel rule obligations

16. What are the benefits and challenges for financial institutions in applying the existing travel rule obligations?

While the existing Travel Rule obligations in Australia do not apply to digital currency exchange providers, we provide the following summary of the benefits and challenges of implementing the Travel Rule from our perspective as a VASP, based on Coinbase's experience in other jurisdictions.

Coinbase supports efforts to apply the Travel Rule to VASPs, as it provides valuable assistance to law enforcement and regulatory agencies in detecting, investigating, and prosecuting money laundering and other financial crimes by creating and preserving an information trail about persons sending and receiving large sums of money through the funds transfer system. But because the Travel Rule was designed many years ago, it understandably does not contemplate digital assets nor does it specifically accommodate for the nuances presented by blockchain technologies. As a result, the Travel Rule construct presents several novel compliance challenges for VASPs.

First, unlike with traditional fiat fund transfers where one can easily identify whether a financial institution is on the other side of a transaction, a permissionless blockchain does not indicate whether a receiving wallet address belongs to a VASP (as opposed to an individual or a different entity). Crypto can be exchanged directly between any two users in a peer-to-peer fashion, without any reliance on an intermediary subject to the Travel Rule. Indeed, ownership of particular wallet addresses is often viewed as highly confidential and subject to strict security measures, due to serious potential business and customer protection risks if those addresses were to be compromised. Thus, before sending sensitive information, a VASP must overcome the challenge of finding a means to confirm whether a VASP is on the other side of a transaction such that the Travel Rule even applies.

Indeed, in many cases counterparty identification itself is not an intrinsic part of crypto transfers; there is no inherent mechanism in the underlying crypto networks/protocols, or a central registry, to identify the owner/control of a receiving address. As it is traditionally applied, the Travel Rule presupposes that a receiving financial institution and beneficiary can be identified as part of the transmittal order and that information can be transmitted to the receiving financial institution with ease. That is not the case with the crypto ecosystem. An originating VASP knows the identity of its own customer, the fiat-equivalent value of the transaction, and the destination address that appears on the blockchain. Yet generally, an originating VASP does not know other details about the transmittal that are relevant to Travel Rule compliance—including whether the recipient address is associated with a VASP. Conversely, a receiving VASP knows the identity of its own customer, the fiat-equivalent value of the transaction, and the originating address that appears on the blockchain. Like

an originating VASP, a receiving VASP generally does not have access to other information relevant to Travel Rule compliance.

Second, even where the originating VASP can accurately determine the identity of the receiving VASP, it must have a method for securely transmitting applicable Travel Rule data. Of course, transmitting this data on-blockchain together with a crypto transmittal would render that sensitive information publicly readable and, in certain cases, is not even feasible for security reasons. The FATF has acknowledged this technical issue and has stated that Travel Rule data does not need to be attached to the crypto transfers itself on the blockchain.[8] Instead, a separate network is needed to enable VASPs to transmit and securely store this data. Given the sensitivity of the information transmitted and shared over such a network, the network must be built to high standards of security and with appropriate governance mechanisms.

Third, the FATF recommends that a VASP send the required Travel Rule information "prior, simultaneously or concurrently with the [funds] transfer itself."[9] For fiat funds transfers through many types of existing systems, such as SWIFT, this requirement is straightforward: the transmittal of value occurs at a readily identifiable point in time, it is clear when the recipient is a financial institution, and there is a technical mechanism enabling the Travel Rule data to be easily transmitted together with a payment instruction.

By contrast, in the context of crypto transfers, this can be more ambiguous for several reasons. A crypto 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 transmittal final and the pace of such confirmations affect how much time is required before the transmittal of value is considered complete. These, in turn, depend on the specific kind of crypto being transferred and the finality standards maintained by the VASP parties to the transmittal, 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 transmittal of value actually occurs (i.e., when the receiving VASP credits the funds) and, accordingly, when Travel Rule data must be provided, may be unclear and will vary depending on the financial institution, though confirmation will still occur within a prescribed time frame.

Coinbase appreciates that the Attorney-General, through this consultation, is taking an effective approach to Travel Rule compliance by directly collaborating with the crypto industry to solve a complex regulatory problem. And the industry has successfully responded to this problem; as mentioned above, Coinbase has worked alongside a large

[8] FATF Oct. 2021 Guidance ¶ 188.
[9] FATF Oct. 2021 Guidance ¶ 185.

group of VASPs over the last few years to pioneer the development of TRUST—a Travel Rule solution that allows VASPs to accurately identify their counterparties and securely exchange required data.[10] We have invested significant legal, compliance, engineering, and other resources to build the TRUST solution, which VASPs 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. All VASPs who join TRUST undergo comprehensive evaluations to help ensure that their security protocols are equipped to prevent unapproved access to sensitive customer data shared by TRUST participants. Further, TRUST was designed so that no customer PII is stored on a centralised database but is instead only shared directly between counterparty VASPs via encrypted, peer-to-peer channels, reducing the risk of hacking or improper access. These 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, and we would be delighted to provide the Attorney-General with more details relating to TRUST.

17. Would the proposed model assist in addressing these challenges?

Coinbase supports the proposed model's suggestion to implement the Travel Rule for VASPs, and also to require payer information to be verified. (For the purposes of this response, we assume that the verification obligation as proposed applies only to the *originating* VASP who holds the contractual relationship with the payer.) However, we suggest that there is nuance in how the Travel Rule is applied, particularly given its global nature, as well as privacy concerns with the potential requirement to collect payee information.

As noted above, the Travel Rule plays a critical role in combating illicit finance. Given the growing role of VASPs in payment flows—both in Australia and elsewhere—applying the Travel Rule to this critical sector will help ensure that crypto assets will be even more

[10] *See* Coinbase, *The Standard for Travel Rule Compliance: Travel Rule Universal Solution Technology*, https://www.coinbase.com/travelrule (describing the TRUST platform and listing VASPs who have joined the TRUST coalition).

difficult for bad actors to exploit. That said, a strict and inflexible application of the Travel Rule to VASPs without the appropriate transition period to allow industry to make the required changes can create challenges. As described above, there are complex technical obstacles to applying the Travel Rule to crypto transfers, which are exacerbated by the differences between jurisdictions in how they apply the Travel Rule to crypto (if at all). The jurisdictional differences are particularly challenging for a technology that is designed to be borderless. These difficulties create uncertainty and place many VASPs at a disadvantage to others—indeed, premature or rushed implementation of the Travel Rule could create a significant competitive disadvantage for Australian VASPs and inhibit innovation.

Offering Australian VASPs a transition period to make the required changes would also align with regulators around the world who have implemented such periods, to ensure that appropriate and compliant Travel Rule Solutions are incorporated. For example, despite FinCEN in the United States stating in 2019 that the Travel Rule applies to VASPs,[11] many U.S. VASPs are still in the process of completing their Travel Rule integrations. Another example is Germany, where the Travel Rule technically came into force in 2021,[12] but multi-year grace periods have been granted to VASPs to complete their integrations. Further, a significant number of countries around the world are either still in the process of finalising their Travel Rule implementation or have yet to begin the drafting process.

We believe that an overly strict application of the Travel Rule to VASPs—for example, by prohibiting VASPs from transmitting funds unless they can transmit Travel Rule data to their counterparty VASP—would unfairly disadvantage Australian VASPs in a manner disproportionate to whatever risks continued transactions may pose. Instead, we submit that the best way forward for the industry is to continue expanding the coverage of Travel Rule compliance solutions while protecting the privacy and security of customers' data and thereby supporting the transitional periods put in place by the global regulatory community.

By contrast, a requirement that VASPs include payee information (as the proposed model suggests) would pose significant concerns and should be reconsidered. In essence, this would require VASPs to affirmatively collect sensitive information about their customer's counterparties (that is, the counterparty name associated with a receiving wallet address) and transmit that information to the receiving VASP. This affirmative obligation to collect and send sensitive data about *non-customers* raises serious privacy concerns, yet provides

[11] *See* U.S. Dep't of the Treasury, Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001, at 11 (May 9, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

[12] *See* Merkle Science, *Germany Mandates Crypto Travel Rule Enforcement Starting 1 October 2021* (Oct. 4, 2021), https://blog.merklescience.com/newsevents/germany-mandates-crypto-travel-rule-enforcement-starting-1-october-2021.

questionable benefit given reliability concerns. For this reason, we recommend against including an affirmative counterparty collection obligation, and to instead follow the approach used in the U.S. Travel Rule, where it is only necessary for VASPs to maintain details on their customer's counterparties *if* counterparty details happen to be received from the VASP's customer as part of a transaction.[13]

The proposed model's affirmative duty on VASPs to collect sensitive information on non-customers would dramatically increase the amount of personal financial data that is collected, stored, and reported by VASPs. Instead of just collecting information on customers with whom a VASP has a contractual relationship, the proposed model would require the collection, storage, and sharing of information on third parties who may never have chosen to be a customer of that VASP, never agreed to any terms covering the use of their financial data, and may not even know their data is being collected and stored in the first place. This is in stark contrast to how information is normally obtained by VASPs. When Coinbase, for example, collects data from its own customers, it does so after its customers voluntarily agree to a disclosed privacy policy and terms of use. By contrast, non-customer counterparties have not agreed to anything with respect to their data. The scale of this proposed expansion in financial data monitoring is significant, as this would result in the collection of granular, transaction-level detail on millions of transactions involving non-customers. In short, the proposed model would turn VASPs into involuntary custodians of massive amounts of non-customer data.

In the face of these large-scale privacy concerns, an affirmative counterparty collection obligation also provides questionable benefit given reliability concerns. VASP customers may not know their counterparty's name, and counterparties may be unwilling—for entirely legitimate reasons—to turn over their sensitive information to customers or VASPs that reach out to them whom they do not know, all leading to high failure rates.[14] Or customers may provide VASPs with incorrect information that is unverified and would now be stored and shared, but actually undermine law enforcement efforts by giving it bad intelligence. Moreover, for transactions between financial institutions, there is no question that the most reliable information about counterparties is held by the recipient VASP where the counterparty is a customer who has been onboarded and verified. Under these circumstances, imposing an affirmative duty on an originating VASP to collect and send counterparty information to a recipient VASP is especially counterproductive and unnecessary.

---

[13] 31 C.F.R. § 1010.410(f)(1) (name, address, and account number of the counterparty are to be retained if "[they] are received with the transmittal order").

[14] Notably, the U.S. Federal Trade Commission warns against providing personal information in response to seemingly legitimate inquiries for much less information. Federal Trade Commission, *Scams and Your Small Business: A Guide For Business* at 3 (May 2018), https://www.ftc.gov/system/files/documents/plainlanguage/ scams_and_your_small_business.pdf ("Remember that email addresses and websites that look legitimate are easy for scammers to fake.").

Given these substantial privacy, data retention, and reliability issues, we recommend against imposing an affirmative duty to collect non-customer counterparty information involving transactions between VASPs. Instead, we recommend adopting the approach used in the existing U.S. Travel Rule where it is only necessary for financial institutions (whether servicing fiat or virtual assets) to maintain details on their customers' counterparties if they happen to be received from the customers.