Select Committee on Australia as a Technology and Financial Centre - Third Issues Paper

Questions taken on notice at Public Hearing

Question 1: If there are opportunities to put certain conditions on participants in place to enhance consumer protection within a regulatory safe space—what would that look like?

Finder recommends an "innovation zone" for the digital asset sector which would offer certainty that there will be no regulatory action arising from the characterisation of digital assets, and related matters where the law is still unclear and clarity that no retrospective actions will be taken once a new framework has been introduced.

Our "innovation zone" proposal goes beyond the "safe harbour" measures proposed by other organisations by also proposing the introduction of some simple requirements for organisations operating within the innovation zone to help protect consumers, give clarity to regulators and to support the policy development work in this space.

Existing consumer protections in the digital asset sector:

Firstly, it is important to note the existing safeguards in Australia that are designed to protect consumers regardless of the sector. The Competition and Consumer Act 2010 already protects consumers against misleading and deceptive conduct[1]. Many of the scams that have occurred in the digital sector contravened this part of the Act and we encourage the ACCC to closely monitor the conduct of the participants in any "innovation zone" that may be introduced.

Similarly, there will be a number of "innovation zone" participants that are also required to comply with the AML/KYC obligations outlined in the Anti-Money Laundering and Counter-Terrorism Financing Act 2006. Again we encourage AUSTRAC to closely monitor the conduct of relevant participants against these laws.

Possible new conditions for participants of the innovation zone:

Beyond these existing protections, there are a number of new conditions that could be placed upon participants in a digital sector "innovation zone". These could include:

[1] https://www.legislation.gov.au/Details/C2013C00620/Html/Volume_3#_Toc368657554

1. **Requiring registration for the innovation zone:**
   Participants within the innovation zone could be required to register for this initiative. This would help regulators to work collaboratively with organisations looking to offer digital asset related products and services in a more controlled environment, while supporting growth in this important sector. This list of registered participants could also be made available to consumers.

2. **Requiring participants to undertake reporting to support policy development**
   Participants in the innovation zone could also be required or asked to report updates to the digital asset regulatory working group on an annual basis. This could include elements such as customer numbers and funds under management to help regulators with market sizing. Careful consideration would need to be given the commercial sensitivity of this data and whether it should be made publicly available but parties could share this with the relevant bodies in confidence. Privacy is another important consideration if this requirement was introduced and participants should have suitable privacy policies and consent mechanisms, and only provide aggregated and anonymised data to ensure each individual's privacy is protected.

3. **Requiring participants to have clear dispute resolution processes**
   Participants in the innovation zone could also be required to meet certain standards in relation to dispute resolution to give consumers a clear course of action if they have a complaint. This is a standard requirement when applying for other licenses or accreditations including the credit license and CDR accreditation that Finder holds currently. This requirement for the innovation zone could include internal dispute resolution procedures that meet existing standards as well as an external dispute resolution process to resolve any unresolved complaints. In the absence of a digital asset focused complaints body, membership of the Australian Financial Complaints Authority (AFCA) could be an option.

4. **Requiring participants to display risk statements or product disclosure statements in relation to innovation zone products / services**
   Participants in the innovation zone could be required to display simple risk statements or create basic product disclosure statements in relation to the products or services offered in the innovation zone. A simple model here could be a generic risk statement message for all products in the space outlining the nature of the innovation zone and the level of regulation present. One parallel is the "warning statement" requirement for short-term loan providers in Australia. This means providers have to follow a consistent format for these warnings including a link to ASIC's MoneySmart website and clearly displaying the National Debt Helpline number. Analysis by ASIC suggests that the "warning statements have been effective at facilitating access to key consumer protection information by a greater range of consumers"[2]. A more

[2]https://download.asic.gov.au/media/3436335/asic-submission-review-of-small-amount-credit-contract-laws-30-october-2015.pdf#page=26

comprehensive version of this could be a specific product disclosure statement for each product or service offered. We would advocate for keeping this statement as simple as possible during the innovation zone phase but should outline the key features, benefits, risks and costs of using a product or service.

Question 2: Does Finder have a view on the travel rule?

The Financial Action Task Force ('FATF') makes recommendations on best practices in avoiding global money laundering and terrorist financing for more than 200 countries and jurisdictions to implement. FATF also publishes Interpretive Notes to their recommendations. The FATF Recommendations 2012 (as amended June 2021)[3] , includes Recommendation 16:

> *Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain. Countries should ensure that financial institutions monitor wire transfers for the purpose of detecting those which lack required originator and/or beneficiary information, and take appropriate measures. Countries should ensure that, in the context of processing wire transfers, financial institutions take freezing action and should prohibit conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373(2001), relating to the prevention and suppression of terrorism and terrorist financing."*

The so-called 'travel rule' is a measure, which mandates that Virtual Asset Service Providers ("VASPs") obtain, hold and exchange information about the originators and beneficiaries of virtual asset transfers.[4] In June 2019, FATF finalised amendments to its global Standards to clearly place anti-money laundering and counter-terrorism financing (AML/CFT) requirements on virtual assets and virtual asset service providers by revising Recommendation 16 (R.16) and adding a new Interpretive Note (INR.15) for the purposes of bringing VASPs under the Wire Transfer recommendations, as follows:

> *"R. 16 – Countries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information on virtual asset transfers, submit the above information to the beneficiary VASP or financial institution (if any) immediately and securely, and make it available on request to appropriate authorities. Countries should ensure that beneficiary VASPs obtain and hold required originator information and required and accurate beneficiary information on virtual asset transfers and make it available on request to appropriate authorities. Other requirements of R. 16 (including monitoring of the availability of information, and taking freezing action and prohibiting transactions with designated persons and entities)*

[3] https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html
[4]https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf

apply on the same basis as set out in R. 16. The same obligations apply to financial institutions when sending or receiving virtual asset transfers on behalf of a customer."[5]

According to FATF, for amounts over the larger of USD/EUR 1000, tracing wire transfers would accomplish the objectives of appropriate law enforcement, enabling financial intelligence, and assisting the reporting of suspicious activity.[6] FATF recommends that:

"Information accompanying all qualifying wire transfers should always contain:
(a) the name of the originator;
(b) the originator account number where such an account is used to process the transaction;
(c) the originator's address, or national identity number, or customer identification number, or date and place of birth;
(d) the name of the beneficiary; and
(e) the beneficiary account number where such an account is used to process the transaction.
7. In the absence of an account, a unique transaction reference number should be included which permits traceability of the transaction."[7]

However, in its *Second 12 Month Review of the Revised FATF Standards on Virtual Assets/VASPS*[8] from June 2021, FATF acknowledges there has been a lack of implementations of the travel rule by jurisdictions.[9] It states *"There was not, however, a technological solution(s) that enabled VASPs to comply with all aspects of the travel rule in a holistic, instantaneous and secure manner when the FATF revised its Standards."*[10]*; and "FATF is not aware yet that there are sufficient holistic technological solutions for global travel rule implementation that have been established and widely adopted".*[11]

The technology powering wire transfers is different to blockchain technology. Wire transfers are typically made within a network of licenced entities, where the method of controlling the transfer is centralised, requires trust and is private. This system is typically used where there is no other option for an individual to transfer funds. Blockchain transfers can be made by individuals as well as VASPs. Transfers are generally trustless, public and recorded on a public blockchain.

We agree with the view that there is currently no workable solution to applying the travel rule to VASPs. Transfers are sent to wallet addresses, which are inherently pseudonymous. There will always be a lack of certainty with trying to link a name to a wallet address as wallet addresses are transferable. If the private key is transferred to another party, the control of the associated address changes. Expecting VASPS to comply without being certain that they can meaningfully comply will stifle innovation in the sector. We also note that digital asset owners would not be personally subject to a 'Travel Rule' and they could simply withdraw the digital asset from the crypto exchange (VASP) and make the transfer themselves to another wallet, which may be to themselves, another individual, or another VASP.

---

[5] Paragraph 7 (b), Page 77, The FATF Recommendations (https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf)
[6] Paragraph 5, page 79 Ibid.
[7] Ibid.
[8] https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf
[9] Paragraph 4, page 2 Ibid.
[10] Paragraph 54, page 17 Ibid.
[11] Paragraph 55, page 18 Ibid.

It is our recommendation that the travel rule should not be applied to Australia at this stage. It would be unworkable from a technological point of view, and more importantly, it is unlikely to achieve the stated objective of tracing digital asset transfers, given the range of avenues to circumvent that are available through both simple and sophisticated means. It has limited application, even if a technological solution is later identified, because digital asset owners can transfer their digital assets privately without using VASPs. We think efforts to tackle money laundering and terrorist financing risks should be focused on the so-called “on and off ramps” for the digital asset sector rather than on digital assets transfers.