Financial
Intelligence Centre

CONSULTATION PAPER

On the implementation of the travel rule for those accountable institutions that engage in crypto asset transfers

INTRODUCTION

1. The Financial Intelligence Centre (Centre) is inviting comments on a draft directive **[link]** to implement the "travel rule" for accountable institutions who are in the business of conducting crypto asset transfers for or on behalf of their clients, as intended by section 43A(7) of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001) (FIC Act). The Centre intends issuing such a Directive in terms of section 43A(2) of the FIC Act.

2. This requirement to implement the travel rule is in line with the anti-money laundering, combating the financing of terrorism and financing of proliferation (AML, CFT and CPF) international standards set by the Financial Action Task Force (FATF).

BACKGROUND

3. The 2014 South African policy position with respect to crypto assets was that crypto assets are largely unregulated in South Africa and that parties engaging in crypto-related activities do so at their own risk and without any regulatory recourse – link to user alert: http://www.treasury.gov.za/comm_media/press/2014/2014091801%20%20User%20Alert%20Virtual%20currencies.pdf.

4. This position has since been revised from the date of publication on 11 June 2021, of a position paper on crypto assets. From June 2021, the South African policy position on crypto assets has been that due to market developments observed over the last few years and the revision of the FATF standards in October 2019, crypto assets can no longer remain outside of the regulatory remit. The position paper on crypto assets published by the Intergovernmental FinTech Working Group (IFWG) – Position Paper on Crypto Assets.pdf (ifwg.co.za).

5. This policy position has developed further. Following the publication of the position paper, the Schedules to the FIC Act were amended and entered into force on 19 December 2022, bringing among others, crypto asset service providers (CASPs) under the remit of the FIC Act by making them accountable institutions under item 22 of Schedule 1. Further, the Financial Sector Conduct Authority (FSCA), in October 2022, declared a crypto asset as a financial product under the the Financial Advisory and Intermediary Services Act, 2002 (Act 37 of 2002) (FAIS Act). Institutions who render financial advisory and / or intermediary services in respect of crypto assets, are required to apply for a license with the FSCA under the FAIS Act. Upon approval of the license,

the institution is also required to register with the Centre as an accountable institution under item 12 of Schedule 1 to the FIC Act. Link to the FIC Act Financial-Intelligence-Centre-Act-2001-Act-38-of-2001.pdf (fic.gov.za) .

6. Members of the IFWG include the following: Financial Intelligence Centre, National Treasury, South African Reserve Bank, Prudential Authority, Financial Sector Conduct Authority, South African Revenue Service, National Credit Regulator and Competition Commission.

THE FINANCIAL ACTION TASK FORCE

7. The FATF is an intergovernmental body that sets standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. South Africa is a member of FATF and of the FATF style regional body, the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) and therefore follows the FATF standards in implementing its measures to combat money laundering and terrorist financing.

8. The FATF standards apply expressly to "virtual assets" and "virtual asset service providers". In the South African context, the IFWG has adopted the terms "crypto assets" and "crypto asset service providers", which are the equivalent to the FATF terminology of "virtual assets" and "virtual asset service providers".

   The FATF definition of "virtual asset" is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. "Virtual assets" do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations. The FATF has confirmed that the definition of "virtual assets" includes so called stable-coins.

9. The FATF definition of "virtual asset service provider" is any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:
   - Exchange between virtual assets and fiat currencies

- Exchange between one or more forms of virtual assets
- Transfer of virtual assets (in this context of virtual assets, transfer means to conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another)
- Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets, and
- Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

10. FATF Recommendation 15 on new technologies reads as as follows:
"Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.
To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations."

The section in red extends the scope of the FATF standards to crypto assets and crypto asset service providers (CASPs).

11. The Interpretive Note to Recommendation 15, clarifies how the FATF requirements apply in relation to crypto assets and CASPs. The interpretive note covers the following: The application of a risk-based approach to crypto asset activities or operations and CASPs; supervision or monitoring of CASPs for AML and CFT purposes; licensing or registration; preventive measures such as customer due diligence, record keeping, suspicious transaction reporting; competent authorities need to take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of a significant or controlling interest, or holding a management function in a CASP; countries should take action to identify natural or legal persons that carry out CASP activities without the requisite licence or registration, and apply appropriate

sanctions and enforcement measures; have a range of effective, proportionate and dissuasive sanctions to deal with CASPs that fail to comply with AML and CFT requirements; ensure the implementation of FATF Recommendation 16 (on wire transfers (in the context of crypto assets it is called the travel rule); and jurisdictions to provide the widest possible range of international co-operation.

12. Consequently, the FATF Recommendations apply to crypto assets and CASPs – just as they apply to financial institutions (such as banks) and designated non-financial businesses and professions (DNFBPs) (such as casinos, estate agents, and legal practitioners).

AMENDMENT OF SCHEDULE 1 TO THE FINANCIAL INTELLIGENCE CENTRE ACT

13. Schedule 1 to the FIC Act was amended with effect from 19 December 2022. One of the amendments included the addition of a new item (item 22) refering to CASPs. The effect of this amendment is that it includes CASPs as accountable institutions, in the scope of the FIC Act. Consequently, CASPs are businesses that must comply with the obligations of the FIC Act. (Further, see paragraph 5 above regarding the FAIS Act and such businesses being accountable institutions under item 12 of Schedule 1 to the FIC Act.)

THE TRAVEL RULE FOR CRYPTO ASSET SERVICE PROVIDERS

14. The travel rule comes from FATF Recommendation 16. The objective of FATF Recommendation 16 is to prevent terrorists and other criminals from having unfettered access to electronically facilitated funds transfers for moving their funds and to facilitate the detection of instances of such misuse when it occurs. The FATF refers to such transfers as “wire transfers.”

15. The functional approach of the FATF is that requirements relating to wire transfers and related messages under Recommendation 16 apply to all providers of equivalent services. This includes CASPs that provide services or engage in activities such as crypto asset transfers that are analogous to wire transfers.

16. FATF Recommendation 16 defines wire transfers as any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary financial

institution, irrespective of whether the originator and the beneficiary are the same person or not.

17. FATF Recommendation 16 applies to CASPs whenever their transactions, whether in fiat or crypto assets, involves:
    - A traditional wire transfer or
    - A crypto asset transfer between a CASP and another obliged entity, for example, between two CASPs, or between a CASP or another obliged entity such as a bank or
    - A crypto asset transfer between a CASP and a non-obliged entity (i.e. an unhosted wallet).

18. The requirements for accountable institutions that engage in these activities, to obtain, hold and submit required and accurate originator and required beneficiary information, are as follows -
    - Accountable institutions that are ordering institutions (originator or sender), whether a CASP or other obliged entity (such as a financial institution), which is involved in a crypto asset transfer, must obtain and hold required and accurate originator information and required beneficiary information and submit the information to beneficiary institutions, where this exists, whether it is a CASP or obliged entity such as a financial institution.
    - Beneficiary institutions (CASP or other obliged entity) must obtain, and hold required (but not necessarily accurate) originator information and required and accurate beneficiary information.

    Required and accurate – meaning verified information.

19. Providers of crypto asset transfers, whether CASPs or other obliged entities, must transmit the required originator and beneficiary information immediately and securely to the beneficiary institution.

20. Immediately means providers must submit the required information prior to, simultaneously or concurrently with the transfer itself. Securely means providers should transmit and store the required information in a secure manner and protect the integrity and availability of the required information to facilitate record keeping and to protect it from unauthorised disclosure.

21. Submission of originator and beneficiary information in batches is acceptable as long as submission occurs immediately and securely. *Post facto* submission of the required information should not be permitted, that is, submission must occur before or when the transaction is conducted.

CONSULTATION

22. Before issuing directives to accountable institutions and other persons regarding their performance, duties and obligations in terms of the FIC Act or any directive made in terms of the FIC Act, the Centre must, in accordance with section 43A(7) of the FIC Act, publish a draft of the directive by appropriate means of publication and invite submissions and consider submissions received.

23. Commentators are invited to comment on the draft directive and questions raised for comment in this consultation paper by submitting written comments to consult@fic.gov.za. Submissions will be received until close of business on Friday, 31 May 2024.

QUESTIONS RAISED FOR COMMENT

TOPIC	QUESTION
A. De minimus threshold for crypto asset transfers	FATF allows jurisdictions to implement a *de minimus* threshold for crypto asset transfers of USD or Euro 1000, having regard to the risks associated with various crypto assets and crypto asset activities. If a threshold is implemented, there are fewer requirements for such transfers below the threshold. These include: - Name of originator and the beneficiary - The crypto asset wallet address or a unique transaction reference number Such information does not need to be verified unless there are suspicious circumstances related to money laundering, terrorism financing or proliferation financing,

	then the information pertaining to the customer should be verified. Should the Directive set out a zero threshold or should a threshold, not exceeding the FATF *de minimus* threshold, be prescribed for crypto asset transfers? What should the threshold be, if a threshold is implemented? Provide reasons.
B. Crypto asset transfers to or from an unhosted wallet	Besides requiring crypto asset service providers to adopt a risk-based approach when dealing with unhosted wallet transfers, and directing them to obtain further information on the unhosted wallet where they have determined, by means of their risk assessments, that there is a higher risk of ML, TF or PF, should the directive set out additional controls that can be implemented for such transactions with unhosted wallets? What could these additional controls be?
C. Crypto asset transfers to or from other crypto asset service providers and counterparty crypto asset service provider identification and due diligence	Paragraph 4.8 of the draft directive sets out that an originator crypto asset service provider must conduct due diligence on their counterparty crypto asset service provider before they transmit the required information and transfers the crypto asset to avoid unknowingly dealing with illicit or sanctioned actors. If the originator crypto asset service provider is not able to conduct the due diligence on the counterparty crypto asset service provider then the originator should not proceed with the transaction. Do you agree with the content set out in paragraph 4.8 of the draft directive? If not, what additional measures should the directive include with respect to this issue?
D. Sunrise issue	Some jurisdictions will require their crypto asset service providers to comply with the travel rule prior to other jurisdictions. Should the directive include the obligation on how crypto asset service providers in compliant jurisdictions

	should deal with crypto asset service providers in jurisdictions not yet compliant with the travel rule? What could these measures include?
E. Privacy coins	Privacy coins are crypto assets which conceal information that could relate to a person to some transaction along with other information such as including the total amount transacted as well as the present balances of wallet addresses. Privacy coins are usually used by people who want their dealings to be anonymous, private and untraceable. Examples include Monero and Zcash. For the purposes of AML, CFT and CPF, it is important to have transparency in respect of transactions. Should the directive prohibit the use of privacy coins in crypto asset transactions by crypto asset service providers or allow such transactions but crypto asset service providers must report such transactions as suspicious transaction in terms of section 29 of the FIC Act?

For more information visit the www.fic.gov.za or contact the Centre's compliance contact centre on +2712 641 6000

Issued by the Acting Director

Financial Intelligence Centre

Private Bag X177

CENTURION

0046