Financial Intelligence Centre

PUBLIC COMPLIANCE COMMUNICATION

DRAFT PUBLIC COMPLIANCE COMMUNICATION

No. 120

GUIDANCE ON THE INTERPRETATION OF CRYPTO ASSET SERVICE PROVIDERS ITEM 22 OF SCHEDULE 1 TO THE FINANCIAL INTELLIGENCE CENTRE ACT, 2001 (ACT 38 OF 2001) AND POTENTIAL RISK INDICATORS

PCC SUMMARY

A "crypto asset service provider(CASP) is listed in item 22 of Schedule 1 to the Financial Intelligence Centre Act, 2001 (Act 38 of 2001) (FIC Act) as "*A person who carries on the business of one or more of the following activities or operations for or on behalf of a client– (a) exchanging a crypto asset for a fiat currency or vice versa; (b) exchanging one form of crypto asset for another; (c) conducting a transaction that moves a crypto asset from one crypto asset address or account to another; (d) safekeeping or administration of a crypto asset or an instrument enabling control over a crypto asset, and (e) participation in and provision of financial services related to an issuer's offer or sale of a crypto asset*".

When considering whether a business is a CASP, the focus is on the economic activities being performed by the business, rather than the technology platform being used, or the specific type of crypto asset being used for the transaction.

This draft PCC provides guidance on the interpretation of item 22 of Schedule 1 and highlights certain money laundering (ML) terrorist financing (TF) and proliferation financing (PF) vulnerabilities that CASPs face.

THE AUTHORITATIVE NATURE OF GUIDANCE

The Financial Intelligence Centre (the Centre) provides the guidance contained in this draft PCC in terms of its statutory function in terms of section 4 (c) of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001) (the FIC Act) read together with Regulation 28 of the Money Laundering and Terrorist Financing Control Regulations (the Regulations) issued in terms of the FIC Act.

Section 4 (c) of the FIC Act empowers the Centre to provide guidance in relation to a number of matters concerning compliance with the obligations in terms of the FIC Act. Guidance provided by the Centre is the only form of guidance formally recognised in terms of the FIC Act and the Regulations issued in terms of the FIC Act. Accordingly, guidance provided by the Centre is authoritative in nature and must be taken into account when interpreting the provisions of the FIC Act or assessing compliance of a accountable or reporting institutions with their obligations as imposed on it by the FIC Act.

It is important to note that enforcement action may emanate as a result of non-compliance with the FIC Act in areas where there have been non-compliance with the guidance has been provided by the Centre. Where it is found that an accountable or reporting institution has not followed guidance which the Centre has issued, the institution must be able to demonstrate that it has nonetheless complied with the relevant obligation under the FIC Act in an equivalent manner.

DISCLAIMER

The publication of a PCC concerning any particular issue, as with other forms of guidance which the Centre provides, does not relieve the user of the guidance from the responsibility to exercise their own skill and care in relation to the users' legal position. The Centre accepts no liability for any loss suffered as a result of reliance on this publication.

COPYRIGHT NOTICE

OBJECTIVE

This draft PCC provides clarity on the practical interpretation and application of a person who carries on the business of a CASP as defined in item 22 of Schedule 1 to the FIC Act.

Further, the draft PCC highlights vulnerabilities faced by a CASP and provides risk indicators and FIC Act compliance obligation guidance that can be considered by a CASP when determining ML, TF and PF risks presented in their client engagements.

1. INTRODUCTION

1.1. CASPs are listed in item 22 of Schedule 1 of the FIC Act as accountable institutions. This PCC seeks to clarify the Centre's interpretation of item 22 of Schedule 1 to the FIC Act.

1.2. Crypto assets are vulnerable to abuse by criminals due to various factors including the cross-border use thereof, the pseudonymous nature of ownership of crypto assets, the ability to transact in non-face-to-face manner. Crypto assets enable anonymous funding (cash funding or third-party funding) through crypto currency exchanges that do not identify the funding source.

1.3. The Centre will supervise and enforce compliance with the FIC Act obligations (anti-money laundering, combating of terrorist financing and combating of proliferation financing) for CASPS in terms of the FIC Act.

2. WHO IS A CRYPTO ASSET SERVICE PROVIDER

2.1. A CASP includes "*a person who carries on the business of one or more of the following activities or operations for or on behalf of a client–*

(a) exchanging a crypto asset for a fiat currency or vice versa;

(b) exchanging one form of crypto asset for another;

(c) conducting a transaction that moves a crypto asset from one crypto asset address or account to another;

(d) safekeeping or administration of a crypto asset or an instrument enabling control over a crypto asset, and

(e) participation in and provision of financial services related to an issuer's offer or sale of a crypto asset".

2.2. The terminology mentioned in this definition is explained further below.

General considerations

2.2.1. **"A person**" which includes both natural persons and legal persons.

2.2.2. "**Carries on the business**" this term is not defined in the FIC Act. The ordinary meaning of the term, within the context of the FIC Act is applied.

2.2.3. **"Business**" this means this person actively carries on a commercial business for profit.

2.2.4. **"Of one or more of the following activities or operations"** this indicates the person could perform either only one of the five activities or operations, or multiple of the activities or operations to meet the definition of being a CASP.

2.2.5. **"For or on behalf of a client"** indicates that a service or product is provided to a client for commercial gain. The definition, therefore, ***excludes*** instances where a person conducts a crypto asset activity in a personal capacity, as opposed to doing so on a commercial basis as a regular feature of their business for clients.

2.2.6. **"Crypto assets"** refers to a digital representation of perceived value that can be traded or transferred electronically within a community of users of the internet who consider it as a medium of exchange, unit of account or store of value and use it for payment or investment purposes, but does not include a digital representation of a fiat currency or a security as defined in the Financial Markets Act, 2012 (Act 19 of 2012).

2.2.7. Stable coins and Non fungible tokens (NFTs) are considered crypto assets for purposes of Schedule item 22.

Specific business activity considerations

2.3. Whether or not a person is categorised as a CASP is dependent upon the activity or operations the person provides and not the use of a particular technology. The emphasis is on the activity or operation provided by the CASP.

2.4. There may be scenarios where other parties play a role in an activity or operation, or the activity or operation might be automatically executed through a computer programme. The person providing the service would be considered a CASP, and not the technology provider.

2.5. Persons fall within the category of CASPs where the person performs one, or multiple of the following five activities or operations for or on behalf of a client:

a) ***"exchanging a crypto asset for a fiat currency or vice versa".***

Example 1

Using a crypto asset exchange platform, A purchases an X crypto coin from ABC crypto exchange for a predetermined rand amount.

Or

The client A pays for the purchase of crypto coin using Rands. The client purchases the crypto coin from CASP X, who operates a business of buying and selling crypto assets through payment of either rands or other fiat currency and vice versa.

b) ***"exchanging one form of crypto asset for another"***

Example 2

CASP A, as one of their services, offers to exchange a whole or a part of X crypto coins for a whole or a part of P crypto coins. Client D wishes to change his P crypto coins to X crypto coins. D proceeds with the exchange transaction with CASP C.

Or

The client A request CASP X to take five B crypto coins in exchange for four E crypto coins. CASP X provides the service to client A at a cost as part of CASP X's business.

c) ***"conducting a transaction that transfers a crypto asset from one crypto asset address or account to another"***

Example 3

E wishes to move his L crypto coins from one of his digital wallets to another and makes use of ABC CASP to do so.

d) ***"safekeeping or administration of a crypto asset or an instrument enabling control over a crypto asset"***

Example 4

F makes use of business G which offers safe holding of crypto assets or the private keys to the crypto asset for or on behalf of their clients.

e) ***"participation in and provision of financial services related to an issuer's offer or sale of a crypto asset"***

Example 5

Business H determines that there will be an initial coin offering*. The business offers their clients and prospective customers financial services (advice or intermediary services) related to the initial coin offfering.

* Refers to a capital raising method where a company sells a crypto asset to an investor.

2.6. Persons that are established, registered, incorporated or licensed in South Africa to provide activities or operations as referred to in these five business activities are required to register as CASPs with the Centre.

2.7. Where parties are engaging in peer-to-peer transactions, neither of the parties would be considered as a CASP unless a party to the transaction provided activities or operations as per the definition of a CASP.

Example 6

Person A sends Person B crypto assets. However, a centralised exchange is not used for this transaction. Neither Person A, nor Person B provide any services as defined in item 22 of Schedule 1, therefore they are not CASPs.

3. COMPLIANCE OBLIGATIONS

3.1. The FIC Guidance Note 7 provides comprehensive guidance on the FIC Act compliance obligations relating to accountable institutions, including CASPs. In addition, the below considerations are highlighted which CASPs should take note of.

Risk-based approach

3.2. As part of the accountable institution's risk-based approach, CASPs must consider the ML, TF and PF risk that correspondent CASPs present, before establishing a business relationship or conducting a single transaction. The following indicators may be considered:

3.2.1. The correspondent CASPs anti-money laundering, countering financing of terrorism and combating proliferation financing (AML, CFT and CPF) regime

3.2.2. The ML/TF risk relating to the correspondent CASP

3.3. CASPs should consider the different ML/TF/PF risks posed by different crypto assets. Various indicators must be considered when determining the level of risk a particular crypto asset presents. These crypto asset indicators that must be considered, include but are not limited to whether the crypto asset:

3.3.1. Provides anonymity

3.3.2. Is easily transferable

3.3.3. Known susceptibility to abuse, trend of misuse.

3.4. In addition to the factors stated in Guidance Note 7 (available on the FIC website www.fic.gov.za), certain unique indicators must be considered by the CASP accountable institution when assessing the level of ML/TF/PF risk a business relationship or single transaction with a client poses (client-level risk assessment). These can include:

3.4.1. Nature and volume of trading of the client

3.4.2. Type of transaction (e.g. to hosted or unhosted crypto wallets etc.)

3.4.3. Source of crypto assets

3.4.4. Client transaction patterns

3.4.5. Crypto asset product risk

3.4.6. Correspondent CASP risk.

3.5. Based upon the risk level, the CASP can determine whether to enter into the business relationship or single transaction, and the level of customer due diligence and monitoring that must be conducted on the client.

Customer due diligence

Below threshold consideration

3.6. Accountable institutions are strongly encouraged to conduct customer due diligence (CDD) on clients where a single crypto asset transaction is below R5 000.00, in the instance where there is a suspicion of ML/TF/PF, and when the funds are going to, or coming from a high-risk jurisdiction, as determined by the CASP.

CDD information and documentation considerations

3.7 Due to the anonymous nature of crypto assets, and the high likelihood that the client and the CASP will never meet on a face-to-face basis, the Centre encourages CASPs to obtain additional information during CDD to ensure adequate identification and verification of their clients. Such information includes, but is not limited to, the client's:

3.7.1 Device identification (including the International Mobile Equipment Identifier (IMEI),

3.7.2 Internet Protocol (IP) addresses

3.7.3 Time stamp

3.7.4 Geo location, and

3.7.5 All Linked crypto asset wallet addresses.

Correspondent CASP engagements

3.8 As accountable institutions, CASPs deal with various other CASPs that are either based in South Africa (and therefore also accountable institutions) or foreign CASPs. Based upon the different types and geographic location of CASPs that the accountable institution deals with, there are differing levels of ML/TF/PF risk that the CASP presents. The accountable institution is encouraged to assess the counterparty CASP's AML/CTF/CPF controls and risk rate them from a ML/TF/PF perspective.

3.9 Where a counterparty CASP presents a heightened ML/TF/PF risk the CASP should determine whether to enter into a business relationship based upon its risk appetite and apply enhanced measures when dealing with such a CASP.

Non-custodial wallet considerations

3.10 Where a customer of the CASP is interacting with a party which has crypto assets in a non-custodial digital wallet, the party is considered to be transacting anonymously. The CASP is still required to CDD. The FIC Act prohibits transacting with anonymous or apparent fictitious clients in terms of section 20A.

Scrutinising a client's information

3.11 CASPs must consider the heightened inherent risk of targeted financial sanctions against designated persons using CASPs in terrorist financing and proliferation financing. Refer to PCC 44 and 54 for further guidance on targeted financial sanctions.

Example 7

Designated persons from high-risk geographic areas such as North Korea misappropriated other people's crypto assets and transfer the crypto assets (through tumblers and mixers) to North Korea, for the purpose of proliferation financing.

3.12 It is recommended that CASPs develop and maintain a list of "bad wallets addresses", that have previously been subject to regulatory reports or negative reports, against which a CASP can screen client information. This includes parties to the transactions, before processing the crypto transactions.

Account monitoring and reporting

3.13 Accountable institutions must monitor all crypto asset transactions to identify suspicious and unusual activity, this includes all crypto-to-crypto transactions as well as crypto to fiat, etc.

3.14 Accountable institutions are advised to develop red-flag indicators which highlight higher risk transactions and scenarios. Where such activity is identified, the

accountable institution must conduct enhanced transactions monitoring. The red-flag indicators must be reviewed on a regular basis to ensure that it is adequate to identify heightened ML/TF/PF risks.

3.15 Possible red-flag indicators, include but is not limited to:

3.15.1 Anonymity characteristics of a crypto asset (e.g. mixers, tumblers etc.)

3.15.2 Transactions based in weak AML/CTF/CPF geographical areas

3.15.3 Transactions patterns are unusual

3.15.4 Transactions that have potential links to dark web

3.15.5 Multiple transactions from the same client over a short period of time. This is known as churning, as it is a method used to conceal the source of illegally obtained funds.

3.15.6 Transactions make no lawful business sense

3.15.7 The beneficiary or originator client profile has unusual or high-risk characteristics

3.15.8 The source of funds or wealth cannot be determined.[1]

3.15.9 Transactions linked to a blacklisted crypto asset address, where it is suspected that they may be involved in ML/TF/PF (with the use of an inhouse, or credible crypto asset data sources of international or domestic blacklisting)

3.16 A CASP must monitor transactions either manually or automatically. Due to the electronic nature and volume of crypto transactions, accountable institutions are strongly encouraged to rely on or implement an automated transaction monitoring system (ATMS) in compliance with Directive 5 as read together with public compliance communication 45.

3.17 The Centre strongly encourages CASPs to include comprehensive transactional information, including transactional hashes, the originators' crypto asset address and recipient's crypto asset addresses when filing reports with the Centre.

[1] FATF Updated Guidance for a risk- based approach: Virtual Assets and Virtual Asset Providers (2021.)

Registration

3.18 Where a person provides multiple product and service offerings against different items under Schedule 1 to the FIC Act, they must register per item. Please refer to PCC 5D for additional examples.

3.19 However, where the person provides multiple service offerings of the five identified business activities set in item 22, the need only register once as a CASP.

4. MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING RISK AND VULNERABILITIES

4.1. The below are examples of areas of vulnerabilities in the CASP industry:

4.1.1. The use of tumblers and mixers. Clients that make use of “tumblers” and “mixers” require additional scrutiny, as they cloud the transaction or undermine the CASPs ability to conduct CDD on their clients or parties to the transaction. This risk consideration should apply to anonymity enhanced cryptocurrency as well.

4.1.2 The anonymous or pseudonymous purchase and sale of crypto assets, lead to heighted risk of obscuring the beneficial owner.

4.1.3 Due to cross-border transactions, and transaction speed being a key characteristic of crypto assets, enforcing and investigating the use of crypto currency for illegal purposes presents challenges. This creates a further layer of difficulty and obscurity and makes it more attractive to criminals.

4.1.4 CASP are exposed to other elements of risk that other accountable institutions may not be exposed to, as bad actors and criminals find crypto assets an attractive alternative to fiat currency.

4.1.5 CASPs can be exposed to associations with elements of the dark web or with bad actors or criminals, with proceeds being derived from ransomware and other case studies.

4.1.6 CASPs are in a unique position in that they have access to all the addresses that are contained in the block chain database. If an address of the block chain for a specific crypto asset is associated with high-risk actors such as known individuals associated with adverse media searches or criminal elements, then subsequent transactions involved in that crypto asset may pose a heighten risk, referred to as “contagious risk.”

4.1.7 The risk of previous owners or parties to the crypto asset is relevant to the current transaction and is referred to as “secondary hops”. An example is where a designated person or entity that sends their crypto asset to an individual presenting a lower risk profile, who within a short time frame transfers their crypto asset to the intended destination of the designated person or entity, in order to conceal or obstruct the party that is the owner of the crypto asset, or the intended beneficiary of the crypto asset.

5. ML/TF/PF RISK STATUS OF A CASP AS AN ACCOUNTABLE INSTITUTION’S CLIENT

5.1. In addition to the principles as set out in Guidance Note 7, it is not considered effective nor adequate risk management if an accountable institution decides to de-risk a client merely because the client is a CASP. It is the Centre’s view that where an accountable institution de-risks solely based upon the fact that a client is a CASP, without regard to any other ML/TF/PF risk factors, then that accountable institution has not complied with its obligation to follow a risk-based approach.

5.2. Where an accountable institution takes the decision to not on board a certain class of clients, the accountable institution must be able to demonstrate the application of a risk-based approach, in terms of which several factors have been considered and not just one (i.e. the fact that clients or prospective clients are CASPs).

5.3. It is the Centre’s view that the accountable institution would have to demonstrate why the ML/TF/PF risk is so high or severe, that the accountable institution does not have appetite to on board a CASP.

5.4. Ineffective application of de-risking can cause inadvertent consequences including the loss of valuable information through regulatory reporting due to the Centre.

6. CONSULTATION

6.1 Before issuing guidance to accountable institutions, supervisory bodies 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 42B of the FIC Act—

6.1.1. Publish a draft of the guidance by appropriate means of publication and invite submissions, and

6.1.2 Consider submissions received.

6.2 Commentators are invited to comment on the draft guidance by submitting written comments via the online comments submission link only. Any questions or requests relating to this draft PCC 120 may be sent to the Centre only at **consult@fic.gov.za**. Submissions will be received until **Friday, 20 January 2023,** by close of business.

7. COMMUNICATION WITH THE CENTRE

7.1 The Centre has a dedicated compliance contact centre geared to assist accountable institutions to understand their registration obligations in terms of the FIC Act. Please call the compliance contact centre on 012 641 6000 and select option 1.

7.2 Compliance queries may also be submitted online by clicking on: http://www.fic.gov.za/ContactUs/Pages/ComplianceQueries.aspx or visiting the Centre's website and submitting an online compliance query.

Issued By:

The Director

Financial Intelligence Centre

15 December 2022