Financial Intelligence Centre

PUBLIC COMPLIANCE COMMUNICATION

PUBLIC COMPLIANCE COMMUNICATION

No. 57

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 transfers 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 asse, where "crypto" means 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).*"

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 public compliance communication (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 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 an 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 which 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.

OBJECTIVE

This 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 PCC highlights vulnerabilities faced by CASPs 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 clarifies 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) (AML, CFT and CPF) of 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,

where "crypto asset" means 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. 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 an item 22 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. There are different types of crypto assets, including but not limited to stablecoins, privacy coins, utility tokens and non-fungible tokens (NFTs) etc. for the purposes of Schedule 1, 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 and not the technology provider would be considered a CASP.

2.5. Persons fall within the category of CASPs where the person performs one, or a 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
The client A purchases crypto assets using rands from CASP X, who operates a business of buying and selling crypto assets.
Or
Client A exchanges crypto assets for rands.

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 asset for a whole or a part of P crypto asset. Client D wishes to change his P crypto asset to X crypto asset. D proceeds with the exchange transaction with CASP C.
Or

The client A requests CASP X to take five B crypto asset in exchange for four E crypto assets. 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 assets 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 offering.

* 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 under Item 22 of Schedule 1.

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

Risk-based approach

3.2. As part of the accountable institution's risk-based approach, CASPs must consider the money laundering (ML), terrorist financing (TF) and proliferation financing (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 AML, CFT and CPF regime

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

3.3. CASPs should consider the ML, TF and 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 CASPs as accountable institutions when assessing the level of ML, TF and PF risk posed by a business relationship or single transaction with a client(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 with the client and assess the level of customer due diligence and monitoring that must be conducted.

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, in the instance where there is a suspicion of ML, TF or PF, and when the funds are going to, or coming from a high-risk jurisdiction, as determined by the accountable institution.

CDD information and documentation considerations

3.7 Due to the anonymous nature of crypto assets, and the likelihood that the client and the CASP will never meet on a face-to-face basis, the Centre encourages CASPs to obtain additional information as part of 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 IMEI – International Mobile Equipment Identifier

3.7.2 Device type and model

3.7.3 Internet Protocol (IP) addresses

3.7.4 Date and time stamp information of device connections

3.7.5 Geo location

3.7.6 Browser information

3.7.7 Operating system and version

3.7.8 All linked crypto asset wallet addresses

3.7.9. A client-provided photograph of themselves (as clients are often requested to take a photograph of themselves when opening an account non face to face).

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 abroad.. Based upon the different types and geographic locations of CASPs that the accountable institution deals with, there are differing levels of ML, TF and PF risk that the CASP presents. The accountable institution is encouraged to assess the counterparty CASP's AML, CTF and CPF controls and risk rate them from a ML, TF and PF perspective.

3.9 Where a counterparty CASP presents a heightened ML, TF and 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 client of the CASP is transacting with a party which has crypto assets in a non-custodial digital wallet, the party is considered to be transacting anonymously, and therefore poses a higher risk of ML, TF and PF, in which scenario the CASP is encouraged to conduct enhanced due diligence on its client.

3.11 CASPs are advised that the requirement to obtain adequate originator and beneficiary information in terms of Recommendation 16 of the Financial Action Task Force will apply to all crypto asset transactions in future. Therefore CASPs are encouraged to adopt controls aimed at compliance with FATF's Recommendation 16.

Scrutinising a client's information

3.12 CASPs must consider the heightened inherent risk of contravention of targeted financial sanctions against designated persons using CASPs in TF and PF. Refer to PCC 54 for further guidance on targeted financial sanctions.

Example 7

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

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

Account monitoring and reporting

3.14 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.

3.15 Accountable institutions are advised to develop indicators which red flag higher risk transactions and scenarios. Where such activity is identified, the accountable institution must conduct enhanced transactions monitoring. The indicators must be reviewed regularly to ensure they are adequate to identify heightened ML, TF and PF risks.

3.16 Possible indicators, include but is not limited to:

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

3.16.2 Transactions based in weak or high-risk AML, CFT and /CPF geographical areas

3.16.3 Rapid or unusual trading patterns, including frequent and rapid buy or sell orders within short time frames, that may suggest market manipulation, wash trading, or other suspicious trading activities.

3.16.4 Transactions that have potential links to Dark Web

3.16.5 Multiple transactions from the same client over a short period of time, referred to as churning, which used to conceal the source of illegally obtained funds.

3.16.6 High-frequency trading as it can be associated with attempts to exploit market inefficiencies or engage in manipulative trading practices, especially when coupled with other suspicious activity.

3.16.7 Transactions that make no lawful business sense

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

3.16.9 The value of the transactions are inconsistent with the client's declared source of income or wealth.

3.16.10 Uncommonly large transactions that are inconsistent with the client profile and transaction patterns

3.16.11 Transactions linked to a blacklisted crypto asset address

3.16.12 Use of money mules, where the criminal operates accounts using the details of a client of the CASP (where client either knows or is unaware thereof), for example, a client provides its CDD information to the CASP and once the account is opened by the CASP, the client then provides the private keys of crypto asset to the criminal.

3.16.13 Online gambling, where a client deposits small amounts to transact with, initiates some minor gambling transactions thereafter withdraws the funds, which then appear to be "legitimate" payouts from the online casino. Where a client's account receives payments from online gambling casinos regularly, this is a red flag, even for small amounts.

3.16.14 Fake social media profiles that market new crypto assets as being profitable or unique, in order to lure clients away from legitimate CASPs. The criminal then misappropriates the fiat or crypto assets without transferring the new crypto assets into the purchasers' wallets.

3.16.15 Social media may also be used to create crypto asset pyramid schemes, which make use of the same principles as the fiat pyramid schemes.

3.16.16 There have been known cases of terrorist organisations posting crypto asset wallet addresses soliciting donations to their cause. An account abruptly receives multiple payments from multiple different crypto addresses or sources, and the crypto assets would be moved out of the account swiftly. Especially if the account is newly created, dormant or low on funds for some time, then this would particularly raise flags.

3.16.17 Where the crypto assets can be purchased through a crypto asset kiosk machine, or automated teller machine with cash, without the client having to open an account. CASPs must conduct CDD on their clients.

3.16.18 Where a client deposits fiat currency into the CASP's account, thereafter advises that the deposit was "made in error" and requests a refund without crypto trading transactions taking place.

3.16.19 Unusually large transactions that are significantly larger than the average or usual transaction size.

3.16.20 The use of multiple accounts and transactions by the same individual or entity. This may indicate attempts to circumvent regulatory limits or conceal illicit activities.

3.16.21 CASPs must pay attention to transactions involving privacy-focused crypto asset types that offer enhanced anonymity features. While these crypto assets types are not inherently illicit, their use in suspicious transactions should raise concerns

3.16.22 Suspicious account access or activity including multiple failed login attempts, account takeovers, or suspicious changes in account information. These indicators may suggest unauthorised access attempts or compromised accounts.

3.16.23 Connections to persons designated on targeted financial sanctions lists, blacklisted wallets or high-risk persons.

3.17. 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 PCC 45.

3.18. In addition, blockchain analysis tools and techniques may be used to trace the flow of funds and identifying patterns that may indicate suspicious and unusual transactions including ransomware payments.

Reporting suspicious and unusual crypto asset transactions to the Centre

3.19. The Centre strongly encourages CASPs to include comprehensive transactional information, including transactional hashes, originators' crypto asset address, the identified wallet, and beneficiary crypto asset addresses with associated wallet identification when filing reports with the Centre.

3.20. There are some common facts that CASPs should include in their reports to the Centre, which include but are not limited to:

3.20.1. Transaction details, including transaction IDs, date and time of the transaction, amounts involved, crypto asset address, wallet identifiers, and any relevant transaction notes or memos.

3.20.2. Client's information, such as the user's full name, contact details, identification documents or any other identifying information provided during the account registration process.

3.20.3. A summary of the client's account activity, including transaction history, account balances, trading patterns, and any additional relevant information.

3.20.4. Address and device information

3.20.5. CASPs should provide their own analysis and assessment of the suspicious activity, highlighting any red flag indicators, unusual patterns, or potential connections to known illicit actors or activities.

3.21. CASPs should include any additional supporting documentation or evidence related to the suspicious transaction. This may include recordings from relevant platform interfaces, communication records with the user, or any other relevant information.

Registration

3.22. 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.

3.23. However, where the person provides multiple service offerings of the five identified business activities set in item 22, they 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 CASP’s ability to conduct CDD on their clients or parties to the transaction. This risk consideration should apply to anonymity enhanced crypto currency 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. Transaction speed and the their cross-border nature are key characteristics of crypto assets, which pose challenges in enforcing and investigating their use for illegal purposes. This creates a further layer of difficulty and obscurity. and makes it more attractive to criminals.

4.1.4. CASP are exposed to elements of risk that other accountable institutions may not be experience, 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 bad actors and criminals, with proceeds being derived from ransomware, the misappropriation of other persons’ crypto assets and other types of crime unique to crypto assets or the digital landscape. In addition, crypto assets are used as a form of exchange for perpetrating other crimes such as fraud, identity theft, Ponzi schemes, romance schemes and other crimes. CASPs should be aware of industry related incidents as, depending on the scale of the crime, this may impact upon their clients as an emerging risk. Most of this information is publicly available through searches for adverse media coverage, and is updated continuously on the internet.

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 a block chain address for a specific

crypto asset is associated with high-risk actors such as known individuals associated with adverse media coverage or criminal elements, then subsequent transactions involved in that crypto asset may pose a heightened risk, referred to as “contagion 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 AND 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 and 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 and 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 which can be filed with the Centre through regulatory reporting.

6. COMMUNICATION WITH THE CENTRE

6.1 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.

6.2 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

3 July 2023