Financial
Intelligence Centre

ASSESSMENT OF THE INHERENT MONEY LAUNDERING AND TERRORIST FINANCING RISKS

CRYPTO ASSET SERVICE PROVIDERS

March 2024

CONTENTS

1. INTRODUCTION

Money laundering can be described as the process whereby criminals attempt to conceal the proceeds of their criminal activities from the actual crime - thereby giving the funds derived from criminal activities an appearance of legitimacy.

Terrorist financing is the process by which individual terrorist and terrorist organisations obtain funds to commit acts of terrorism, which can be done using legally obtained or illicit funds.

Crypto Asset Service Providers (CASPs) is one of the sectors identified by the international anti-money laundering and countering the financing of terrorism (AML/CFT) community as potentially highly vulnerable for money laundering and terrorist financing (ML/TF).

(It must be noted that the Financial Actions Task Force, in its documentation and research papers, refer to "Virtual Assets" and "Virtual Asset Service Providers". In south Africa, the terms crypto assets" and "crypto asset service providers" were adopted for the same products/services.)

The Financial Intelligence Centre (FIC) conducted a risk assessment of the inherent ML/TF risks of CASPs in South Africa. Because there is generally a shortage of reliable and publicly available statistics on the number and value of crypto asset payments processed by payment service providers, participants, merchants and consumers in South Africa, an assessment of the risks and the impact on the financial sector and the broader economy is challenging.

The Financial Sector Conduct Authority (FSCA) published a document "South Arica's Crypto Assets Market Study", wherein it mentioned that the crypto economy in Sub-Saharan Africa is the smallest among all regions, accounting for 2.3% of the global transaction volume from July 2022 to June 2023, amounting to $117.1 billion in on-chain value.[1]

Irrespective of this relatively small uptake of crypto assets, compared to the rest of the world, it must be noted that the sector has made significant inroads in Africa. Nigeria ranked second on

[1] The 2023 Geography of Cryptocurrency Report

the 2023 Chainalysis Global Crypto Adoption Index[2] Other countries in the region that score high on the index include Kenya (21), Ghana (29), and South Africa (31). Furthermore, a 2022 study by Triple A (Singapore Blockchain company) indicates that over 5.8 million people, 9.44% of South Africa's total population, currently own crypto assets, with 43% of the population expected to be using them by 2030.

The FIC and the FSCA amended legislation and published regulations to bring crypto assets under their respective regulatory frameworks. The legislation and regulations seek to achieve financial integrity and consumer protection objectives. However, regulatory gaps may still exist at all appropriate spheres of governance and law enforcement, given that crypto assets impact various policy areas, e.g., efficiency, financial stability, safety and soundness, transparency, financial inclusion, terrorist financing, money laundering and competition.

It is envisaged that this sector risk assessment, although based on a desktop monitoring assessment and research on the sector risks would provide valuable insights to CASPs by promoting greater awareness and understanding of the inherent ML/TF risks to CASPs, as well as by developing methods to reduce and mitigate these risks. While it is understood that the ML and TF environment may change over time, the ML and TF risks drawn from the information obtained and incorporated into this sector risk assessment report are nonetheless important for the sector, the FIC and the FSCA.

[2] The 2023 Geography of Cryptocurrency Report

2. SCOPE, LIMITATIONS AND METHODOLOGY OF THE RISK ASSESSMENT

This sector risk assessment report addresses principally the inherent ML and TF risk factors facing CASPs pertaining to products, services, clients, transactions, delivery channels and geographical areas, as well as terrorist financing risks and the potential mitigation of these risks by complying with the FIC Act.

Although it is recognised that these risks could be mitigated to a degree by introducing policies, processes, procedures and controls in accordance with the requirements of the FIC Act, details of such mitigation factors were not included in this report. The report focuses on inherent risks.

3. LEGISLATIVE REQUIREMENTS AND MARKET OVERVIEW OF THE SECTOR

3.1. Regulation of the sector

3.1.1. In terms of Schedule 1, Item 22 of the FIC Act, CASPs are defined as businesses that:

- *Exchange crypto assets for fiat currencies or vice versa;*
- *Exchange one form of crypto asset for another;*
- *Conduct transactions that move crypto assets from one crypto asset address or account to another;*
- *Provide facilities for the safekeeping or administration of crypto assets or instruments that enable the control of crypto assets;*
- *Participate in or provide financial services related to issuers' offers or sale of crypto assets.*

3.1.2. In October 2022, the FSCA issued a draft declaration of crypto assets as a 'financial product' in terms of the Financial Advisory and Intermediary Services Act, 2002 (Act No. 37 of 2002) (FAIS Act). The declaration requires CASPs to be licenced for provision of advisory and intermediary services in respect of crypto assets. This introduces regulatory oversight and may assist in addressing the immediate exploitation of consumers by unscrupulous entities.

3.1.3. The Declaration has the effect that any person who, as a regular feature of their business, renders financial services (as defined in section 1 of the FAIS Act to include advice and/or intermediary services) in relation to crypto assets, must:

- either be authorised under section 12 of the FAIS Act as a financial services provider (FSP);
- or be appointed as a representative of an authorised FSP under section 13 of the FAIS Act;
- and comply with the requirements of the FAIS Act and its subordinate legislation.

3.1.4. The FIC and the FSCA will jointly supervise and enforce compliance with the FIC Act obligations (AML/CFT) and countering proliferation financing (CPF)) for CASPS in terms of the FIC Act.

3.2 Market overview of the sector

3.2.1 The number of CASPs that are registered with the FIC under Item 22 of Schedule 1 of the FIC Act, totaled 87 on 20 February 2024. Although this does not confirm the total number of operators, it provides an indication of the size of the sector in South Africa.

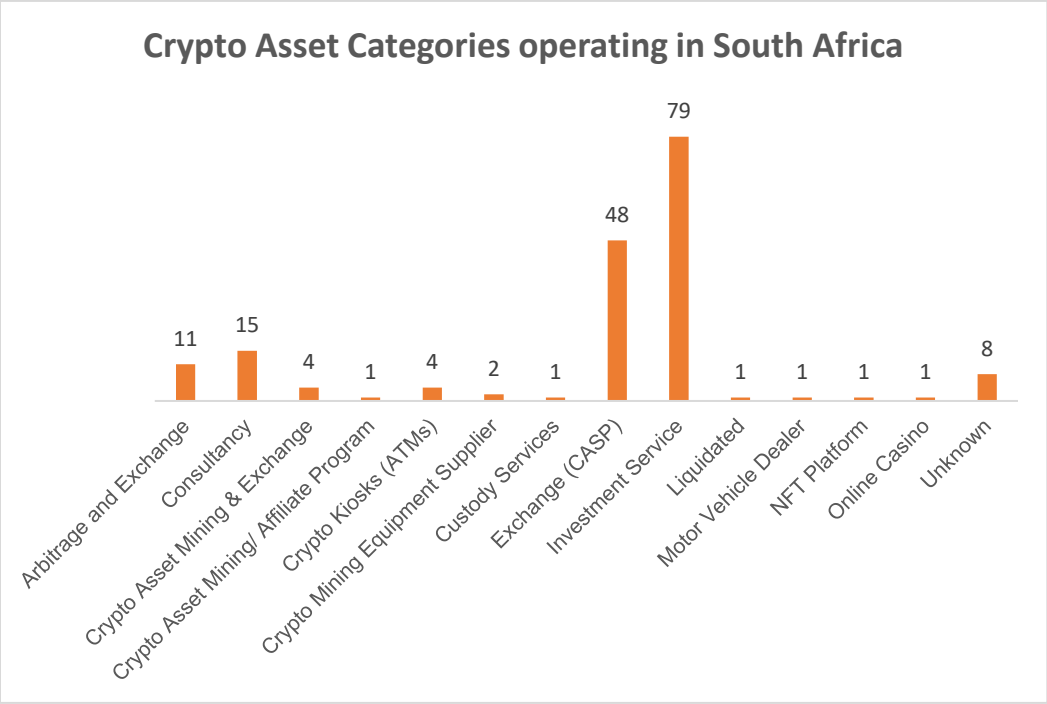
3.2.2 Based on available statistics, it was estimated that over 5,8 million people (9.44%) of South Africa's total population, currently own crypto assets. Calculating the total value of these crypto assets is a challenge and due to the rapid changes in ownership, such information may not be accurate. Research that was conducted indicates that men in the age category of 18 to 34 are more likely to own crypto currencies.

3.2.3 The FSCA, in its report on crypto assets, indicated that the average crypto assets traded were approximately R520 million per month in 2022. They have also established that 60% of Financial Services Providers (FSPs) who provide services in respect of crypto assets, do so in relation to unbacked crypto assets while 26% provide such services in relation to stablecoins. This study also indicates that 54% of FSP providing services in respect of crypto assets have 100% of their business built around retail customers. This is an indication that the emphasis is mainly on the extension of ownership of crypto assets among retail investors.[3]

[3] South Africa's crypto assets markets study by the FSCA

3.2.4 Breaking down crypto asset ownership by income, it is noted that 77% of South African crypto asset owners have an annual income of R450 000,00 and less. This suggests that crypto assets are largely owned by low to middle income South Africans.

3.2.5 Marketplaces as registered business entities were categorized as follows as part of the crypto asset ecosystem in South Africa:



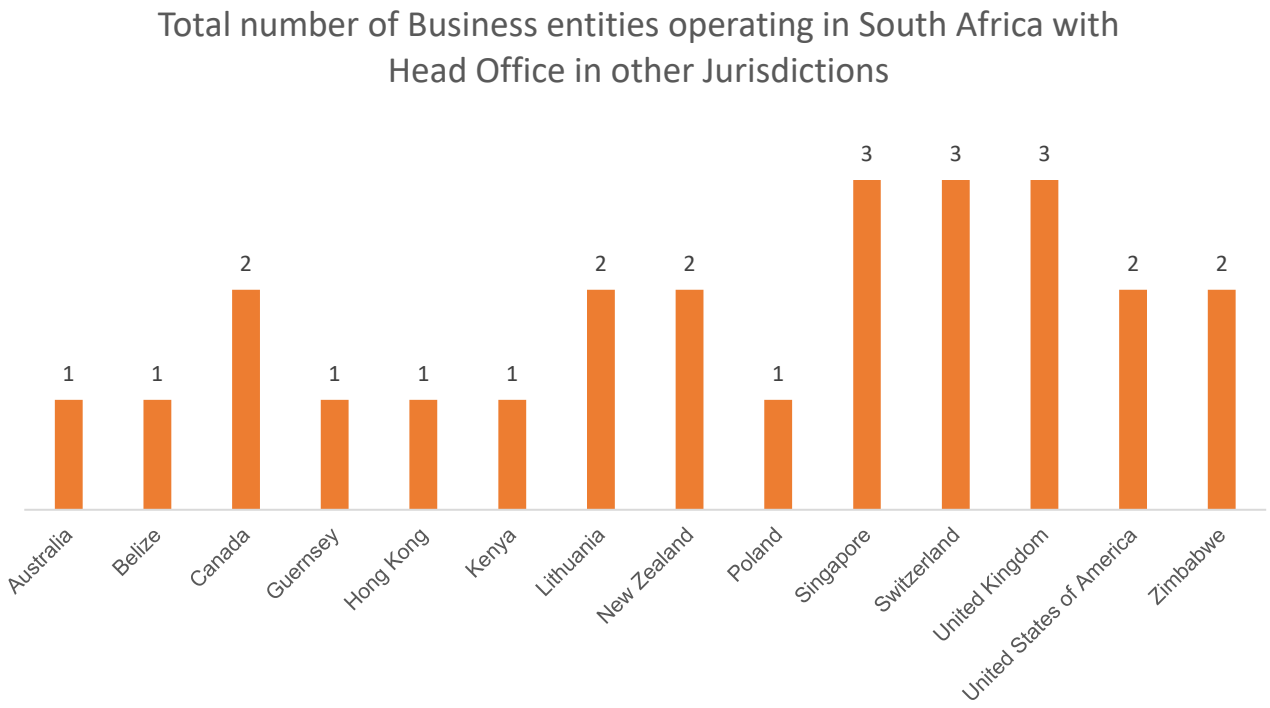
It was observed that the crypto asset markets consist mainly of CASPs (48) and Investments services (79):[4] This is an indication that, although crypto assets are not as yet regularly used and accepted in the broader economy of South Africa, there is an increase in exchanging fiat currency for crypto assets and it is also increasingly used as an investment vehicle. This may be as a result of investors starting to realise the potential for growth in the value of crypto assets over the longer term, notwithstanding potential large fluctuations over the short-term.

3.2.6 Some of the identified business entities have Head Offices in other jurisdictions, whilst they also operate in South Africa. Some of the local business entities also operate Internationally,

[4] Information based on research by Compliance and Prevention Division of the FIC

which could possibly increase the geographic ML/TF/CPF risks due to the differences in supervision and statistical information available.

Statistics on local and international services operating in South Africa are as follows:[5]



This table illustrates the international footprint of the South African CASP sector and the potential of the sector to engage in cross-border transactions, thereby contributing to the potential money-laundering and terrorist financing risks of the sector.

3.3 Key market drivers

- Growing Interest in crypto assets:

  The interest in crypto ecosystems is steadily increasing among South Africans. The demand for CASPs and other supporting services increased as people sought alternative investment opportunities and digital assets. There may be various reasons for such growing interest in crypto assets as an alternative investment, such as:

  - Crypto assets can be seen as a hedge against inflation, although the volatility of crypto assets is in itself a significant risk, it may be seen as an alternative

[5] Information based on research by Compliance and Prevention Division of the FIC

for other assets that has been subject to potential decreases in value due to, e.g. higher inflation and currency depreciation.

- The decentralized nature of crypto assets resonates with some who see it as a way to bypass traditional financial institutions and achieve greater financial inclusion.
- Crypto assets can facilitate faster and cheaper cross-border payments, which can be attractive for individuals with family or business interests abroad.
- Some individuals are drawn to the potential for high returns offered by certain crypto assets.

- Financial Inclusion:

  South Africa has a large unbanked and underbanked population. Crypto assets offered a means for financial inclusion, attracting users who didn't have access to traditional banking services.

- Regulatory Clarity:

  Regulatory clarity is emerging in South Africa, which is seen as a positive sign for the crypto industry. Regulatory frameworks provide a level of legitimacy and security for CASPs, encouraging their growth.

- Fintech Innovation:

  South Africa has a burgeoning fintech ecosystem. Many startups and established financial institutions are exploring blockchain technology and crypto assets, creating opportunities for CASPs to collaborate and provide services.

- Remittances:

  Crypto assets could be used for cross-border remittances due to their lower fees and faster transaction times compared to traditional remittance services.

3.4 **Challenges**

- Regulatory Uncertainty:

  While regulatory clarity is improving, the crypto industry still faces challenges related to regulatory uncertainty. Changes in regulations could have a significant impact on CASPs, and they need to stay agile and adapt to new rules.

- Security Concerns:

  The crypto industry is vulnerable to security breaches and hacking incidents. Examples of such security breaches and hacking include:

- Ransomware - where sensitive business is the target and encrypted. To release the data, crypto assets are then demanded for the decryption keys.
- Advanced fee fraud and non-delivery scams are on the rise where crypto assets are being used by criminals.
- Crypto romance scams are also on the rise. This is a deceptive investment fraud that targets individuals through romantic relationships or online friendships. Scammers gradually build trust with their victims over time before manipulating them into investing in fake crypto platforms.

CASPs needed robust security measures to protect their customers' funds and data.

- Lack of Consumer Awareness:

  Many South Africans are not fully familiar with crypto assets, or the services offered by CASPs. Education and awareness campaigns are necessary to onboard new users.

- Banking Relationships:

  CASPs often faced difficulties in establishing and maintaining banking relationships. Some banks in South Africa were found to be reluctant to provide services to crypto-related businesses, making it challenging to operate smoothly.

- Market Volatility:

  Although some crypto assets in South Africa are linked to other assets, the inherent volatility of crypto assets still posed challenges for CASPs. Price fluctuations could affect their profitability and risk management strategies.

- Competition:

  The crypto industry is becoming increasingly competitive, with new CASPs entering the market regularly. Established players have to innovate to maintain their market share.

- Scams and Fraud:

  The crypto industry is susceptible to scams and fraudulent activities. CASPs need to implement strong due diligence and compliance measures to mitigate these risks.

4. THE INTERNATIONAL MONEY LAUNDERING RISKS AND TERRORIST FINANCING RISKS ASSOCIATED WITH CASPs

4.1 It is evident from actions that were introduced internationally that the ML and TF risks of crypto assets and crypto asset service providers has been recognised some time ago.

The FATF has already in 2018 included crypto assets and crypto asset service providers as part of institutions to which AML and CTF measures should apply.

4.2 FATF stated in its "Updated guidance for a risk-based approach for Virtual assets and virtual asset service providers", that was published in October 2021, as follows:

"In October 2018, the Financial Action Task Force (FATF) adopted changes to its Recommendations to explicitly clarify that they apply to financial activities involving virtual assets; FATF also added two new definitions to the Glossary: "virtual asset" (VA) and "virtual asset service provider" (VASP). The amended FATF Recommendation 15 requires that VASPs be regulated for anti-money laundering and countering the financing of terrorism (AML/CFT) purposes, that they be licensed or registered, and subject to effective systems for monitoring or supervision.

In June 2019, the FATF adopted an Interpretive Note to Recommendation 15 to further clarify how the FATF requirements should apply in relation to VAs and VASPs, in particular with regard to the application of the risk-based approach to VA activities or operations and VASPs; supervision or monitoring of VASPs for AML/CFT purposes; licensing or registration; preventive measures, such as customer due diligence, recordkeeping, and suspicious transaction reporting, among others; sanctions and other enforcement measures; and international co-operation."

4.3 FATF Recommendation 15 under the heading "New technologies" reads 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."

4.4 The crypto-asset market structure fosters vulnerabilities. Investment and activity in the crypto asset market is largely self-contained and is mostly for speculative purposes with limited connections to the real economy. Many intermediaries, particularly trading and lending platforms, have sought to grow rapidly by advertising high returns and investing in risky products provided by other intermediaries. Such a business strategy relies upon an ongoing increase in the price and value of crypto-assets or an inflow of new investment to meet its obligations. Some lending platforms have also sought to generate yield by extending concentrated loans to large crypto-asset market participants. These business models have generated extensive and complex financial relationships. Like traditional finance, high yield is most often achieved by taking greater credit risks, greater liquidity/maturity mismatches or more leverage.

4.5 Due to the pseudonymity or anonymity of crypto-asset market participants, many intermediaries require "over-collateralisation" in crypto-asset margin trading and lending as a substitute for creditworthiness screening. This may result in a lack of customer due diligence (CDD) measures of the borrower as a result of the lender being covered by the higher collateral and not being too concerned to obtain additional information on the borrower. However, given the high volatility of crypto-assets, sharp declines in asset values may occur, reducing the value of collateral and potentially triggering margin calls or collateral liquidation. In such cases, the high degree of interconnectedness in the crypto-asset market may lead to cascades of liquidations, contributing to the propagation and amplification of risk contagion and market strains.

5. REPORTING BY CASPs UNDER THE FIC ACT

5.1. The volume of reports received from CASPs:

CASPs were brought into the ambit of the FIC Act on 19 December 2022 which placed an obligation to submit regulatory reports (except for section 29 reporting that is applicable to all businesses). The reporting statistics are low due to the reporting statistics period available. CASPs filed a total of 3 cash threshold reports (CTRs) and 151 suspicious transaction reports (STRs) between 19 December 2022 and the end of

the financial year of the FIC on 30 March 2023. No terrorist property reports (TPRs) were submitted during this time.

5.2. Types of reports filed

CASPs registered with the FIC have an obligation to file regulatory reports in terms of section 28, section 28A and section 29 of the FIC Act. Most regulatory reports submitted to the FIC by CASPs are STRs, filed in terms of section 29 of the FIC Act. The sector's reporting trends indicates the fact that cash is not prevalent in the sector.

6 RISKS BASED ON DESKTOP MONITORING AND RESEARCH

The risk factors used in this report align with those used in the FIC's Guidance Note 7, issued by the FIC and is available on www.fic.gov.za, and also includes a reference to terrorist financing risk.

CASPs need to consider these factors when conducting their daily business:

6.1 Products and services risks

Organised criminals have learned to perfect the process of digital money laundering, which typically follows these stages:

Crypto money-laundering stages

- **Entry** - Criminals buy a basic cryptocurrency, often via an intermediary with clean records and corroborated employment. They then further distance themselves from the purchase by using pseudo-anonymous e-wallets, adopting pseudonyms, and using log-less virtual private networks (VPNs) and blockchain-optimised smartphones.
- **Conversion** - Once the purchase has been verified, fiat currency is used to place funds to buy primary coins, such as Bitcoin. These are then used to purchase altcoins at an advanced exchange. Certain altcoins offer an enhanced level of anonymity.
- **Masking** - Criminals then use mixing services such as Bitmixer to swap primary coin addresses for temporary digital wallet addresses to trick the blockchain and disrupt audit traceability.

- **Washing** - Next, criminals' layer numerous privacy coins, exchanges and digital addresses to effectively cleanse their illicit funds for reintegration into the traditional financial system.
- **Withdrawal** - Criminals finally withdraw cleansed funds, typically using one of these methods:

In a process known as burst-out integration, privacy coin holdings are traded for primary coins and then to a basic currency which can be sent to a connected bank account. Digital holdings are transferred to a hardware crypto wallet or printout of a QR code which can be sent anywhere in the world.

6.2 Client risks

Listed as accountable institutions under the FIC Act, CASPs are required to assess, identify, understand and then risk-rate the inherent money laundering and terrorist financing risks associated with their clients. Some clients, such as foreign politically exposed persons (FPEPs), domestic politically exposed persons (DPEPs,) domestic prominent influential persons (DPIPs), complex legal structures or foreigners potentially pose a higher risk for money laundering, depending on the identified circumstances.

CASPs should be aware of, inter alia, the following possible scenarios pertaining to the nature and behaviour of the clients that could point to possible money laundering:

Source of Funds

- Sources of crypto assets can be potentially tied or directly linked to illicit activity. For example, funds may be transacted from a platform with little-to-no AML or Know Your Customer (KYC) regulations in place, a possible red flag about the origin of the funds.
- Similarly, a single crypto wallet could be tied to multiple banks and credit cards, denoting a group of people, acting as "mules" and using one wallet to move funds around.

In addition to this, the FATF also mentions the red flags indicators below that specifically relate to the sources of funds and / or wealth. This was published by the FATF in September 2020 in its document "Virtual Asset Red Flag Indicators of Money laundering and Terrorist financing" and uses the term "Virtual Assets" (Vas):

- Transacting with VA addresses or bank cards that are connected to known fraud, extortion, or ransomware schemes, sanctioned addresses, darknet marketplaces, or other illicit websites.
- VA transactions originating from or destined to online gambling services.
- The use of one or multiple credit and/or debit cards that are linked to a VA wallet to withdraw large amounts of fiat currency (crypto-to-plastic), or funds for purchasing VAs are sourced from cash deposits into credit cards.
- Deposits into an account or a VA address are significantly higher than ordinary with an unknown source of funds, followed by conversion to fiat currency, which may indicate theft of funds.
- Lack of transparency or insufficient information on the origin and owners of the funds, such as those involving the use of shell companies, or those funds placed in an Initial Coin Offering (ICO) where personal data of investors may not be available or incoming transactions from online payments system through credit/pre-paid cards followed by instant withdrawal.
- A customer's funds which are sourced directly from third-party mixing services or wallet tumblers.
- Bulk of a customer's source of wealth is derived from investments in VAs, ICOs, or fraudulent ICOs, etc.
- A customer's source of wealth is disproportionately drawn from VAs originating from other VASPs that lack AML/CFT controls.

The FATF also identifies the following red flag indicators relating to anonymity of clients, but also stated that it must not in all instances be seen as red flag indicators on its own, but should be considered in conjunction with other risk factors:

- Transactions by a customer involving more than one type of VA, despite additional transaction fees, and especially those VAs that provide higher anonymity, such as anonymity-enhanced cryptocurrency (AEC) or privacy coins.
- Moving a VA that operates on a public, transparent blockchain, such as Bitcoin, to a centralised exchange and then immediately trading it for an AEC or privacy coin.
- Customers that operate as an unregistered/unlicensed VASP on peer-to-peer (P2P) exchange websites, particularly when there are concerns that the customers handle huge amount of VA transfers on its customer's behalf and charge higher fees to its

customer than transmission services offered by other exchanges. Use of bank accounts to facilitate these P2P transactions.

- Abnormal transactional activity (level and volume) of VAs cashed out at exchanges from P2P platform-associated wallets with no logical business explanation.
- VAs transferred to or from wallets that show previous patterns of activity associated with the use of VASPs that operate mixing or tumbling services or P2P platforms.
- Transactions making use of mixing and tumbling services, suggesting an intent to obscure the flow of illicit funds between known wallet addresses and darknet marketplaces.
- Funds deposited or withdrawn from a VA address or wallet with direct and indirect exposure links to known suspicious sources, including darknet marketplaces, mixing/tumbling services, questionable gambling sites, illegal activities (e.g. ransomware) and/or theft reports.
- The use of decentralised/unhosted, hardware or paper wallets to transport VAs across borders.
- Users entering the VASP platform having registered their Internet domain names through proxies or using domain name registrars (DNS) that suppress or redact the owners of the domain names.
- Users entering the VASP platform using an IP address associated with a darknet or other similar software that allows anonymous communication, including encrypted emails and VPNs. Transactions between partners using various anonymous encrypted communication means (e.g. forums, chats, mobile applications, online games, etc.) instead of a VASP.
- Many seemingly unrelated VA wallets controlled from the same IP-address (or MAC-address), which may involve the use of shell wallets registered to different users to conceal their relation to each other.
- Use of VAs whose design is not adequately documented, or that are linked to possible fraud or other tools aimed at implementing fraudulent schemes, such as Ponzi schemes.
- Receiving funds from or sending funds to VASPs whose CDD or know-your-customer (KYC) processes are demonstrably weak or non-existent.
- Using VA ATMs/kiosks –
  - despite the higher transaction fees and including those commonly used by

mules or scam victims; or

- in high-risk locations where increased criminal activities occur.

A single use of an ATM/kiosk is not enough in and of itself to constitute a red flag but would if it was coupled with the machine being in a high-risk area or was used for repeated small transactions (or other additional factors).

6.3 Transaction risks

Criminal groups or individuals could transfer multiple times without a commercial explanation, begging the question about why those transactions are taking place.

Other suspicious patterns may include:

- High-frequency transactions of large sums from many wallets into one account during a single period.
- Structuring of transactions (e.g. exchange or transfer) in small amounts, or in amounts under record-keeping or reporting thresholds, like structuring cash transactions
- High value transactions in a short time period or in a staggered and regular pattern or to a newly created or previous inactive account
- Transferring crypto assets immediately to multiple service providers, especially to service providers registered or operated in another jurisdiction where there is no relation to where the customer lives or conducts business; or there is non-existent or weak AML/CFT regulation.
- Depositing crypto assets at an exchange and then often immediately withdrawing the crypto assets without additional exchange activity to other crypto assets, which is an unnecessary step and incurs transaction fees, converting the crypto assets to multiple types of crypto assets - again incurring additional transaction fees, but without logical business explanation (e.g. portfolio diversification) or withdrawing the crypto assets from a service provider immediately to a private wallet.
- Crypto wallets that do not match customer profiles.
- Fast transfer of deposits from regulated jurisdictions into unregulated jurisdictions
- Peel chain transactions. This is a technique used to launder large amounts of unlawfully obtained crypto assets by funding a long series of small transactions. These small transactions often involve small amounts of crypto currency, and CASPs are often used for peel chain transactions.

6.4 Risks relating to delivery channels

CASPs must be aware of the delivery channels they use to attract and deal with clients. Delivery channels that may obscure or conceal the true identity of the client, or that result in clients not being on-boarded face-to-face, may increase the risk of being abused by criminals to launder the proceeds of crime. Where an intermediary is used to on-board clients, the sector must do proper due diligence on the intermediary and its business and must be familiar with the risk-mitigation processes and procedures the intermediary may have in place.

CASPs are advised to clearly highlight and explain the terms and conditions of conducting business on their trading platforms or on social media and to include all the necessary control measures in such terms and conditions to minimize the possibility of it being abused by criminals.

There have been known cases where criminals had stolen other client's money through a CASP, and they opened an account with a subsequent CASP that did not verify their identity before opening their account. It was due to this error by the CASP that a further layer of transactions was added to funnelling the proceeds and making the investigation by law enforcement agencies more difficult. This emphasises the importance of conducting identification and verification when non-face-to-face delivery channels are used, as non-face to face is more likely to be used in the CASP industry.

6.5 Geographic risk

Some foreign jurisdictions pose a higher risk for money laundering. It is important that CASPs be aware of the risks posed by clients from these jurisdictions and that they have the necessary risk mitigation processes in place. In some geographical areas, there is a fraction of the amount of AML or KYC regulations needed. This, alongside a lack of full implementation of preventive measures (e.g. the "travel rule") and/or the existence of regulatory bodies, creates opportunities that can be exploited by criminal groups.

In higher-risk jurisdictions, users will potentially see a larger amount of suspicious transaction patterns or dubious fund sources. Due to the relative lack of protections for legitimate traders, these areas should be avoided.

Similarly, there have been instances of crypto asset service providers that have been liquidated as a result of poor governance procedures, and possible money laundering in an attempt for the company to remain viable especially where there have been fluctuations in the crypto asset share price. A possible reason for this is that these companies are still emerging, and there is much potential in this industry. There have been several cases of directors or senior managers of crypto asset service providers that have been fined or even sentenced to imprisonment. CASPs should be mindful of adverse media, especially where it involves other CASPs in the industry.

CASPs must be aware of the potential higher risks posed by clients and counterparties from the following types of countries, including:

- That are subject to a travel ban.
- Which the FATF regards as a high ML risk
- That are regarded as high secrecy jurisdictions.
- Which are regarded as “tax havens”.
- Where they are known to have high levels of organised crime, corruption or from which terrorist organisations are known to operate.

The globalised nature of crypto assets allows for customers that are international in scope. This also allows for possible criminals from other countries to penetrate the CASP’s software and misappropriate crypto assets of other clients. There is further appeal due to crypto assets being able to be converted into the foreign criminal’s specific currency. As a result, this specific industry must consider international crime syndicates which may not be as prevalent in other sectors.

6.6 Terrorist financing risk

In October 2015, the FATF released a report entitled “Emerging Terrorism Financing Risks,” which specifically analyzed the terrorist financing risks of crypto assets. This report highlighted that some crypto assets have increasingly become “accomplices” to various illegal and criminal activities, facilitating money laundering and terrorist financing. Terrorist financing based on emerging technologies can allow terrorist organizations to instantly transfer funds worldwide. However, it also increases the difficulty of counterterrorist financing in relevant countries. Virtual assets may be used to finance terrorism. Owing to the decentralization and anonymity features

of crypto assets, illegal transactions cannot be regulated. The Federal Reserve and European Central Bank have warned crypto assets are highly speculative in nature and are used in illegal financing activities.

Terrorist organizations may use crypto assets due to the following three main reasons.

- First, crypto assets are generally characterized by the anonymity of transactions and the free cross-border flow of funds. Hence, terrorists can easily conceal the source and location history of their funds. Terrorists may also find circumventing foreign exchange quotas and regulations on foreign exchange remittances abroad easy.

- Secondly, as the identity of the crypto asset owner is encrypted in the crypto asset network, people can only identify the source, flow direction, and circulation mode of the crypto asset with the identity of the crypto asset owner still unknown.

- Thirdly, the “convertibility” of crypto assets allows terrorists to turn crypto assets into fiat currency. Simultaneously, the decentralized nature of crypto assets also provides an opportunity for terrorists to escape bank and government supervision, enabling them to quickly transfer funds without formal financial institutions knowing.

An emerging trend that has come to light is where terrorist groups appeal to the public to donate to their wallet address directly. This would be either in the guise of donating for humanitarian causes in areas of conflict, or even to donate to the terrorist groups themselves. The advertisement would be through social media, where the address of their wallet is provided.

CASPs must know how to access the referenced targeted financial sanctions list and determine whether they are conducting business with individuals and institutions on such lists. The United States’ “Office of Foreign Assets Control” have started to incorporate the “blacklisting” of known crypto asset addresses that have been used in terrorist financing or have been affiliated with terrorist groups.

6.7 Proliferation financing risk

Due to high-risk geographic countries being subject to financial sanctions, and with the globalized nature of crypto assets, Democratic People's Republic of Korea (DPRK) has been known to use operators to gain access to CASPs and misappropriate crypto assets of other customers to and use money laundering methods to funnel such misappropriated funds towards the proliferation financing program in DPRK.

Like the combating of terrorist financing, targeted financial sanctions are also used to combat proliferation financing. CASPs must know how to access the referenced targeted financial sanctions list and determine whether they are conducting business with individuals and institutions on such lists. Designated persons for proliferation financing appear on the targeted financial sanctions list in addition to the terrorist financing list.

7. INDICATORS OF MONEY LAUNDERING AND TERRORIST FINANCING ACTIVITY FOR THE SECTOR

The following could be regarded as ML/TF vulnerabilities and risks associated with CASPs.

- Technological features that increase anonymity – such as the use of peer-to-peer exchanges websites, mixing or tumbling services or anonymity enhanced cryptocurrencies;
- Sender or recipient profiles – unusual behaviour can suggest criminal activity;
- Lack of ML/TF awareness of the CASPs;
- High-risk customers and jurisdictions, such as clients linked to institutions or jurisdictions on the sanctions lists;
- Payments from non-associated or unknown third parties and payments for fees in cash where this practice is not typical;
- Cryptocurrencies facilitate cross-border transactions while bypassing the controls of traditional financial institutions.
- Funds are received from or sent to a foreign country when there is no apparent connection between the country and the client;

- Instances where clients, for no apparent reasons change the way in which transactions are concluded or change their instructions to the legal practitioners on short notice or in a manner that does not make economic sense;
- Cryptocurrencies have many legitimate uses, but they also attract launderers because these transactions can be anonymous, fast, automated and global in nature, making it more difficult (and in turn take more time) for law enforcement agencies to trace the proceeds of the crypto assets being moved.

In addition to the above, FATF, in its "Virtual Assets Red Flag Indicators" document, also refers to the following red flags relevant to the profile and unusual behaviour of either the sender or the recipients of crypto assets:

<u>Irregularities observed during account creation</u>

- Creating separate accounts under different names to circumvent restrictions on trading or withdrawal limits imposed by VASPs.
- Transactions initiated from non-trusted IP addresses, IP addresses from sanctioned jurisdictions, or IP addresses previously flagged as suspicious.
- Trying to open an account frequently within the same VASP from the same IP address.
- Regarding merchants/corporate users, their Internet domain registrations are in a different jurisdiction than their jurisdiction of establishment or in a jurisdiction with a weak process for domain registration.

<u>Irregularities observed during CDD process</u>

- Incomplete or insufficient KYC information, or a customer who declines requests. for KYC documents or inquiries regarding source of funds.
- Sender / recipient lacking knowledge or providing inaccurate information about the transaction, the source of funds, or the relationship with the counterparty.
- Customer has provided forged documents or has edited photographs and/or identification documents as part of the on-boarding process.

Profile of potential money mule or scam victims

- Sender does not appear to be familiar with VA technology or online custodial wallet solutions. Such persons could be money mules recruited by professional money launderers, or scam victims turned mules who are deceived into transferring illicit proceeds without knowledge of their origins.
- A customer significantly older than the average age of platform users opens an account and engages in large numbers of transactions, suggesting their potential role as a VA money mule or a victim of elder financial exploitation.
- A customer being a financially vulnerable person, who is often used by drug dealers to assist them in their trafficking business.
- Customer purchases large amounts of VA not substantiated by available wealth or consistent with his or her historical financial profile, which may indicate money laundering, a money mule, or a scam victim.

8. CONCLUSIONS

8.1 The new FATF Recommendations aim for effective regulation of CASPs, the crucial interface between the sphere of crypto assets and fiat currencies. Therefore, AML/CTF standards that apply to traditional financial transactions should, in as far as possible, also cover blockchain-based financial services. Ultimately, the plan is to put an end to anonymous virtual transactions. The wire transfer rule, also called the ‘Travel Rule’, requires states to take precautions to ensure that CASPs monitor and share customer data among themselves and with the relevant government authorities.

8.2 Crypto advisors often claim that laundering money with crypto assets is highly complex and risky, making it an ineffective strategy compared to conventional techniques. They also argue that transactions in digital currencies are more transparent and accountable compared to fiat currencies. Another argument is: money laundering using crypto assets is comparatively very small in terms of volume and mainstream media is focusing more on criminal activities related to digital currencies rather than technology and innovation. Albeit on a small scale, there is no doubt that crypto assets are being used to facilitate money laundering.

8.3 There should be proper tools to verify the identity of people who transact in crypto assets. They should be able to match and relate blockchain transactions with real identities, creating an end-to-end trail to help with AML investigations. Transaction monitoring tools that dig out suspicious patterns for further investigations are also essential for the AML compliance programmes of crypto.

8.4 Crypto assets can provide added anonymity for cybercriminals, and most crypto exchanges and CASPs currently operate with significantly less regulatory scrutiny and can be used to circumvent international borders. But while crypto assets may provide some advantages over traditional methods of money laundering, the technology is also publicly recorded and publicly accessible – making each and every transaction traceable. This includes crypto wallets that were used in commission of previous crimes, and which is publicly available. Similarly, there are “blacklisted” crypto asset addresses that have been blacklisted by certain regulatory authorities which are publicly available as well.

8.5 To manage and mitigate the risks emerging from virtual assets, countries should ensure that CASPs 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.

8.6 At this stage, due to the potential for abuse and the fact that mitigating supervisory measures are still in the process of being introduced, the overall inherent risk of money laundering and inherent terrorist financing risk for the CASPs sector in South Africa, based on national and international experience, can be classified as high. The sector will however be monitored, and it is also envisaged that it will be subject to further supervisory oversight, which may impact the ML/TF risk rating of the sector in future.