Financial
Intelligence Centre

ASSESSMENT OF THE MONEY LAUNDERING AND TERRORIST FINANCING RISKS

CRYPTO ASSET SERVICE PROVIDERS

1 April 2025

CONTENTS

1. INTRODUCTION

1.1 Money laundering can be described as the process whereby criminals attempt to conceal the proceeds that result from their criminal activities and from the actual crime(s), thereby giving the funds derived from criminal activities the appearance of legitimacy and being able to enjoy the fruits of their criminal activities.

1.2 Terrorist financing is the process by which individual terrorists and/or terrorist organisations obtain funds through legitimate or illicit means, to commit acts of terrorism.

1.3 One of the sectors identified by the international anti-money laundering and combating of terrorist financing community as being particularly vulnerable conduits for money laundering and terrorist financing is the crypto asset service provider (CASP) sector.

1.4 The international body for setting standards on combating money laundering, terrorist financing and proliferation financing, the Financial Action Task Force (FATF), refers to crypto assets as virtual assets and the sector as virtual asset service providers. In South Africa, the Crypto Assets Regulatory Working Group (CAR WG) (a working group under the Intergovernmental Fintech Working Group) adopted the terms “crypto assets” and “crypto asset service providers” (CASPs).

1.5 The Financial Intelligence Centre (FIC) conducted an assessment of the money laundering and terrorist financing (ML and TF) risks facing CASPs in South Africa and have also referred to the combating of the proliferation financing risk in the South African context.

1.6 Due to the scarcity 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.

1.7 The *2024 Geography of Cryptocurrency* report, published by Chainalysis states that: "Sub-Saharan Africa accounts for the global cryptocurrency economy's smallest share, representing 2.7% of transaction volume worldwide between July 2023 and June 2024 — a reflection of the region's smaller aggregate gross domestic product relative to other regions. Nonetheless, Sub-Saharan Africa saw modest growth, receiving an estimated $125 billion in on-chain value during this period (July 2023 to June 2024), a $7.5 billion increase compared to the previous year."

1.8 Irrespective of the relatively small use of crypto assets compared to the rest of the world, the sector has made significant inroads in Africa between July 2023 and June 2024. Nigeria maintained its position as a top global player, ranking second worldwide, while Ethiopia (26), Kenya (28), and South Africa (30) also made the top 30 worldwide.[1] Furthermore, a 2022 study by Triple A (a Singapore Blockchain company) indicates that over 5.8 million people in South Africa, 9.44 percent of South Africa's total population, at that stage owned crypto assets, with 43 percent of the population expected to be using them by 2030.

1.9 Effective from 19 December 2022, the sector was listed as item 22 in Schedule 1 of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001) (FIC Act). This meant that from that date, CASPs were required to fulfil FIC Act compliance obligations including registration and regulatory reporting to the FIC. The amendments to the legislation seek to strengthen financial integrity and consumer protection objectives. However, regulatory gaps may continue to exist at all appropriate spheres of governance and law enforcement, given that the use of crypto assets impact various policy aspects including efficiency, financial stability, safety and soundness, transparency, financial inclusion, terrorist financing, money laundering and competition.

1.10 It is envisaged that this sector risk assessment, although based on desktop monitoring assessment and research, would provide valuable insights by promoting greater awareness and understanding of the ML and TF risks to CASPs, as well as by articulating methods to reduce and mitigate these risks. CASPs should use this report to develop and apply such methods in their day-to-day AML/CFT risk management. While

[1] The 2024 Geography of Cryptocurrency Report

the ML and TF environment may change over time, the risks inferred from the information obtained and incorporated into this assessment report are nonetheless important for the sector, the FIC and FSCA.

2. SCOPE, LIMITATIONS AND METHODOLOGY OF THE RISK ASSESSMENT

2.1 This sector risk assessment report addresses the ML and TF risk factors facing CASPs pertaining to products, services, clients, transactions, delivery channels and geographical areas.

2.2 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 domestic legislative framework (including the FIC Act and Financial Advisory and Intermediary Services Act, 2002 (Act 37 of 2002) (FAIS Act)), details of such mitigation factors are not included in this report.

3. LEGISLATIVE REQUIREMENTS AND MARKET OVERVIEW OF THE SECTOR

3.1. Regulation of the sector

3.1.1. CASPs are defined in Item 22 of Schedule 1 of the FIC Act as businesses that provide one or more of the following activities or operations for or on behalf of a client:

- *Exchange a crypto asset for a fiat currency or vice versa*
- *Exchange one form of crypto asset for another*
- *Conduct a transaction that transfers crypto asset from one crypto asset address or account to another*
- *The safekeeping or administration of crypto assets or instruments that enable the control over a crypto asset*
- *Participation in or provision of financial services related to issuers' offers or sale of a crypto assets.*

3.1.2. In October 2022, FSCA issued *General Notice 1350 of 2022*, declaring crypto assets as a 'financial product' in terms of the FAIS Act. The declaration required CASPs to be licensed for the provision of advisory and intermediary services in respect of

crypto assets. This introduced regulatory oversight and is aimed at assisting in addressing the immediate exploitation of consumers by unscrupulous entities.

3.1.3. The declaration entails 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
- Comply with the requirements of the FAIS Act and its subordinate legislation.

3.1.4. As financial services providers registered under the FAIS Act, CASPs are also included as accountable institutions as envisaged in the description of item 12 of Schedule 1 to the FIC Act, for which FSCA is the designated supervisory body. In addition, CASPs must also register under item 22 of Schedule 1 of the FIC Act where it relates to the activities mentioned in this item, for which the FIC is the designated supervisory body. The FIC and FSCA jointly supervise and enforce compliance with the FIC Act obligations (AML, CFT and CFP) for CASPs in terms of the FIC Act.

3.2 Market overview of the sector

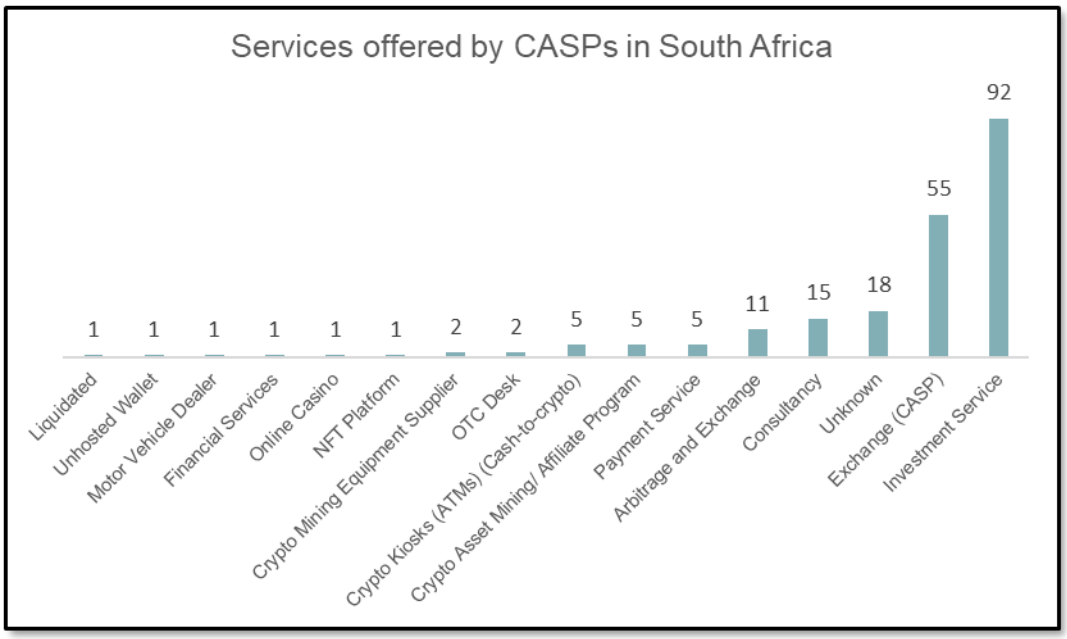
3.2.1 As of 10 February 2025, the total number of CASPs registered with the FIC under item 22 of Schedule 1 of the FIC Act, was 256. It must however be noted that this may not be a true reflection of the size of the sector in South Africa, as there may be institutions operating without being registered with the FIC.

3.2.2 Based on available statistics, it is estimated that more than 5.8 million people (9.44 percent of South Africa’s total population) currently own crypto assets. Calculating the total value of these crypto assets is challenging, and due to the rapid changes in ownership, such information may not be accurate.

3.2.3 In its report on crypto assets[2], the FSCA indicated that, on average, approximately R520 million in crypto assets were traded per month in 2022. The FSCA also established that 60 percent of financial services providers (FSPs) who provide crypto asset services, do so in relation to crypto assets not backed by physical or financial assets and 26 percent in relation to stablecoins. Their study also showed that 54 percent of FSPs providing crypto asset services had 100 percent of their business built on retail customers. This was a clear indication that the emphasis was mainly on the extension of ownership of crypto assets among retail investors.[3]

3.2.4 Research conducted by the FIC in 2023 indicates that, at the time, 77 percent of South African crypto asset owners had an annual income of R450 000 and less. This suggests that crypto assets are largely owned by low to middle income South Africans.

3.2.5 The table below shows the breakdown of different services offered by CASPs in South Africa and is based on research by the FIC, using open-source information.



2 https://www.fsca.co.za/Documents/Crypto%20Market%20Study.pdf#search=crypto%20report

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

The FIC observed that, in 2023, the crypto asset market in South Africa consist mainly of CASPs (55) and investment services (92).[4] While generally there appears to be low level use of crypto assets in South Africa, the statistics indicate that crypto is increasingly being used as an investment vehicle. This may be as a result of investors starting to realise potential for growth in the value of crypto assets over the longer term, notwithstanding potential large fluctuations over the short term. Stablecoins, backed by the US dollar is also increasingly being used as a hedge against exchange fluctuations by investors in crypto assets.

Case study 1, presented in Annexure A below, provides additional information on market developments in the South African context.

3.2.6 Some of the identified business entities have head offices in other jurisdictions, while they also operate in South Africa. Some local business entities also operate internationally, which could possibly increase geographic ML and TF risks due to the differences in supervision.

The FIC's statistics show that twenty-five (25) South African business entities have their head offices in other jurisdictions, whilst also conducting business in South Africa. Of these jurisdictions, Singapore, Switzerland and the United Kingdom are each home to three head offices of institutions also operating in South African.

3.3 Findings from 2024 Financial Intelligence Centre report

3.3.1 The difficulty of determining statistics and obtaining information in this ever-changing sector is evident from the fact that, in a study that was based on information up to 28 June 2024, the FIC has found that at least five institutions had an internet presence in South Africa but were not registered with the Companies and Intellectual Property Commission (CIPC). Three of these five were also not registered with the FIC or the FSCA. This report also identified 12 institutions that are registered with CIPC (but not with the FIC) that do not have an internet presence in South Africa and in which no

[4] Information based on research by Monitoring and Analysis Division of the FIC

financial activities were detected. A further three CIPC registered institutions were identified as having operated through international social media platforms.

3.3.2 The 2024 FIC report also referred to unconfirmed information relating to 31 institutions, allegedly involved in activities ranging from investment services, crypto mining, crypto kiosks and exchanges which were not registered with the FIC or the FSCA. In addition, the report also generated transactional risk indicators, using the local CASPs transaction histories across all chains in which the indicators were categorised as Severe risks (involving transactions associated with crimes such as child sex abuse, TF and sanctions), high risks (involving transactions linked to e.g. banned substances, darknet markets, illicit goods and malware), medium risks (involving transactions linked to e.g. decentralised gambling, investment services and Ponzi schemes) as well as low risks (involving transactions linked to e.g. lending services and mining). This analysis indicated that nine CASPs were associated with the transactions in the “severe risks” group as well as the “high” group, while a further four were associated with transactions in the “high” risks group.

3.4 Key market drivers

- **Growing interest in crypto assets:**

  The interest in crypto ecosystems is steadily increasing among South African consumers or users. The demand for CASPs and other supporting services increased since 2021 as people sought alternative investment opportunities in 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 to other assets that are subject to potential decreases in value due to e.g. higher inflation and currency depreciation.
  - The decentralised 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 offer a means for financial inclusion, attracting users who do not have access to traditional banking services.

- **Regulatory clarity:**

  Regulatory clarity has emerged in South Africa during the last three years, 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.

- **Transaction freedom:**

  Crypto assets allow for borderless and decentralised transactions. Investors appreciate the freedom to transfer funds globally without relying on traditional banking systems.

- **Inflation:**

  In jurisdictions with high inflation rates, an investment in stablecoins that is linked to strong currencies, such as the US dollar, can potentially provide a hedge against depreciations in local currency.

3.5 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. While the money laundering and terrorist financing risks have technically been addressed by legislative changes, such legislative changes in respect of exchange control are still in the planning phase. The lack of proper exchange control measures for crypto assets may also negatively impact on the money laundering and terrorist financing risks associated with crypto assets.

- **Security concerns:**

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

  - Ransomware: – Where sensitive businesses and some government departments, are targeted through social engineering, exploitation of lax or poor security measures and other means. Through ransomware, the cyber criminals encrypt the business or public entities' data. To release the data, crypto assets are demanded in exchange for decryption keys. Businesses in South Africa are still improving their cyber security measures and as a result this trend is on the rise.
  - Advanced-fee fraud and non-delivery scams – where victims are asked to pay fees upfront in return for products or services: Criminals are increasingly using crypto transactions in these crimes.
  - 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.
  - Transactions with sanctioned entities. Due to the global nature of crypto assets, entities designated on a targeted financial sanctions (TFS) list use crypto assets as a payment method to evade sanctions, and to continue operating.
  - CASPs need to have robust security measures in place to protect their business, and their customers' funds and data.

- **Lack of consumer awareness:**

  Many South Africans are not fully acquainted with crypto assets, or the services offered by CASPs. Consumers need to be made aware of the use, storage and

transfer value of crypto assets, and any concerns need to be addressed. Consumers also need to be informed about how they can fall victim to organised crime using them as money mules. (Refer to *Financial Crime insights: Money laundering risks associated with money mules*, published by the FIC).

- **Challenges relating to law enforcement agencies:**
  Crypto assets are still a relatively new reality and law enforcement agencies and criminal investigators would need to, over time, improve their knowledge and technical skills relating to these assets to be able to also improve investigations into crimes committed using these assets.
- **Banking relationships:**
  In the past, CASPs have in some instances found it difficult to establish and maintain banking relationships. Some banks in South Africa were initially found to be overly cautious and reluctant to provide services to crypto-related businesses, making it challenging to operate smoothly. Although it has improved, this could potentially make it difficult for CASPs to offer consumers with a facility to convert crypto assets into fiat and *vice versa* through bank account transfers, leading to alternative methods of conversion.
- **Market volatility:**
  Although some crypto assets in South Africa are linked to other assets, such as the US dollar, the inherent volatility of crypto assets still poses challenges for CASPs with price fluctuations potentially affecting their profitability and risk management strategies.
- **Competition:**
  The crypto industry is becoming increasingly competitive in South Africa, with new CASPs entering the market regularly. Established players must innovate to maintain their market share.
- **Financial crimes, including scams and fraud:**
  The crypto industry is susceptible to scams and fraudulent activities – mainly due to the potential for anonymity with some transactions. CASPs need to implement strong due diligence and compliance measures to mitigate these risks. Examples of such tools are blockchain analytics, geolocation tools, and coin risk assessments.

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

4.1 In 2018 FATF included CASPs – which they referred to as virtual asset service providers – as institutions to which member countries needed to apply anti- money laundering (AML) and combating the financing of terrorism (CFT) measures.

4.2 FATF stated in its *Updated guidance for a risk-based approach for virtual assets and virtual asset service providers*, 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:

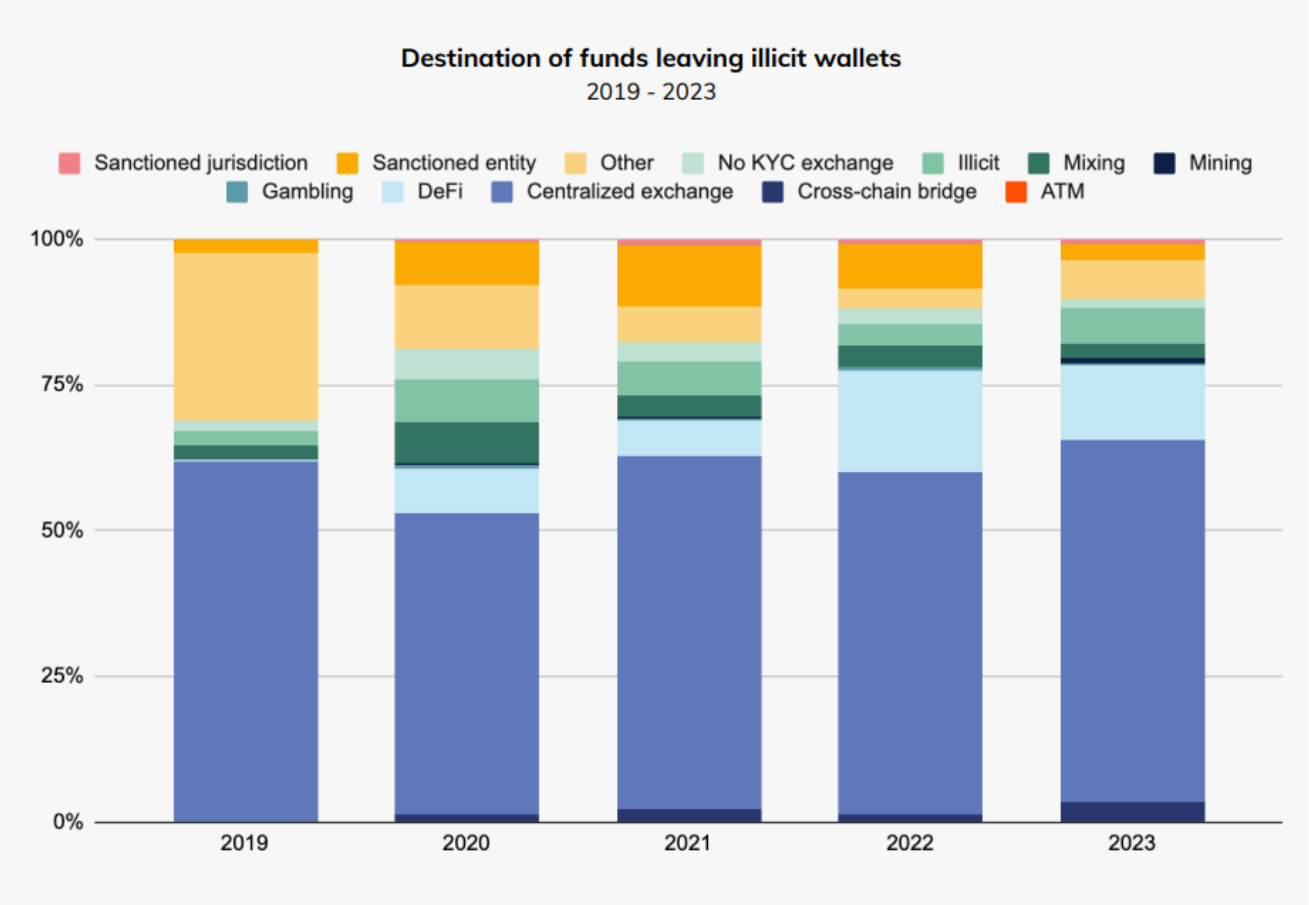
"*Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both 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 In its 2024 *Crypto Crime Report*, blockchain analysis firm Chainalysis focused on two services and on-chain entities in its analysis of crypto money laundering, namely intermediary services and wallets as well as services facilitating the exchange of fiat currency for crypto and *vice versa*. Crypto criminals use intermediary services such as the provision of wallets, tumblers and mixers (where potentially tainted crypto assets are mixed with others) and instant exchangers to obfuscate their criminal origins, often obscuring the on-chain link (where transactions occur on a blockchain) between their source address and current address. Services that facilitate the exchange of crypto to fiat currency, such as centralised exchanges, P2P exchanges and crypto ATMs may also be abused by criminals to obscure the origins of funds.

4.5 The graph below, from the Chainalysis report, depicts the destination of funds worldwide from illicit wallets and shows that such funds predominantly go to centralised exchanges. Other destinations that show an increase are funds send to blockchain bridges where value is transferred from one blockchain to another as well as funds send to gambling platforms. It must be noted that in Sub-Saharan Africa centralised exchanges are by far the most popular platform for crypto transactions, facilitating over half of all crypto transactions. This increases the risk of funds from illicit wallets flowing to the region.



4.6 The Chainalysis report also examined the exchange deposit addresses and concluded that in 2023, 109 exchange deposit addresses worldwide received more than US$10 million worth of crypto currency and collectively received US$3.4 billion in illicit crypto currency. This illustrates that the flow of illicit crypto assets is still, to a large extent, concentrated to a small number of exchanges (although less so than in the previous year which reflected that only 40 exchange deposit addresses received over US$10million, for a collective total of just under US$2 billion).

4.7 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 increasing credit risks and liquidity, maturity mismatches or leverage.

4.8 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 customer due diligence (CDD) measures not being applied upon the borrower as a result of the lender being covered by the higher collateral and not being too concerned about obtaining 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 instances, 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 as a new item (item 22) in Schedule 1 of the FIC Act which obliged them to register with and submit regulatory reports to the FIC. Section 29 reporting is applicable to all business, and as such, CASPs were under an obligation to submit such reports even before 19 December 2022. The reporting statistics are low due to the reporting statistics period available. CASPs filed a total of 43 cash threshold reports (CTRs) and 7 248 suspicious and unusual transaction reports (STRs) during the 2023/24 financial year (between 1 April 2023 and 31 March 2024). 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 sections 28, 28A and 29 of the FIC Act. The majority of 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 indicate that cash is not prevalent in the sector, although it is still used to a limited extent.

6 RISKS BASED ON DESKTOP MONITORING AND RESEARCH

The risk factors used in this report align with those in the FIC's Guidance Note 7A which 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

6.1.1 Organised criminals have gained expertise in the process of digital money laundering, which, although not unique to the crypto asset environment, typically follows the stages below when involving crypto assets:

Crypto money laundering stages

- **Entry** – Criminals buy a basic crypto asset, often via an intermediary who has a clean record and can corroborate their employment status. They then further distance themselves from the purchase by using pseudo-anonymous digital 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 private coins at an advanced exchange. Certain private coins offer enhanced levels 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 clean their illicit funds for re-integration into the traditional financial system.
- **Withdrawal** – Criminals finally withdraw cleaned funds, typically using one of these methods:

6.1.2 In a process known as burst-out integration, privacy coin holdings are traded for primary coins and then to fiat 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.

6.1.3 Crypto transactions emanating from decentralised financing and direct transactions such as peer-to-peer transactions, may pose a higher risk for money laundering and terrorist financing and CASPs should make arrangements to make further enquiries on such transactions when appropriate and must be able to identify and assess the ML and TF risks associated with their different products.

6.2 Client risks

6.2.1 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 and/or clients transacting from foreign countries, potentially pose higher risks for money laundering and terrorist financing, depending on the identified circumstances.

6.2.2 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.

6.2.3 In addition to this, FATF also mentions the red-flag indicators below that specifically relate to the sources of funds and/or wealth. FATF published these indicators 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 for 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 historical transactions associated with the client, while there may also be an unknown source of funds, followed by conversion to fiat currency, which may indicate suspicious behaviour.
- 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 there are incoming transactions from online payments system through credit or 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 and CFT controls.

6.2.4 FATF identified the following red-flag indicators relating to anonymity of clients but also stated that not all instances were to be seen as red-flag indicators on their own. Instead, they 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 crypto currency (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 or unlicensed VASP on peer-to-peer (P2P) exchange websites, particularly when there are concerns that the customers handle huge amounts of VA transfers on their underlying customer's behalf and charge higher fees to their customers 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 bridges, 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 or tumbling services, questionable gambling sites, illegal activities (e.g. ransomware) and/or theft reports.
- The use of decentralised or "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 the owners of the domain names.
- Users entering the VASP platform using an IP address associated with darknet or other similar software that allows anonymous communication, including encrypted e-mails and VPNs. Transactions between partners using various anonymous encrypted communication means such as forums, chats, mobile applications and online games 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 processes are demonstrably weak or non-existent.
- Using VA ATMs or kiosks –
    - Despite the higher transaction fees and including those commonly used by mules or scam victims
    - In high-risk locations where increased criminal activities occur.

6.2.4 A single use of an ATM or kiosk is not enough in itself to constitute a red flag but would be so if coupled with the ATM being in a high-risk area or being used for repeated small transactions (or other additional factors). According to the latest figures from “coinatmradar.com” there are nineteen (19) bitcoin ATMs in South Africa, of which six (6) are in Durban, seven (7) in Johannesburg and four (4) in Cape Town and one (1) each in Pretoria and Gqeberha. The legality of bitcoin ATMs is under consideration by FIC and FSCA.

6.3 Transaction risks

6.3.1 Criminal groups or individuals could transfer multiple times without a commercial explanation, which would lead to the question about why those transactions are taking place.

6.3.2 Other suspicious patterns may include:

- High-frequency transactions of large sums from many wallets addresses 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 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 operating in another jurisdiction where there is no relation to where the customer lives or conducts business; or there is non-existent or weak AML and 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 series of small transactions. These transactions often involve small amounts of crypto assets, and CASPs are often used for peel chain transactions.

6.3.3 With the increased acceptance of crypto assets, and with technology allowing almost anyone to be able to create a crypto asset, there is an emerging trend where the developers of a crypto asset project suddenly abandon their project, taking all of the funds invested by users with them (also referred to as a “rug pull.") This is particularly the case with new lesser-known coins. The crypto asset developers initially promise above market returns, on social media or sporting events, and there is little economic reason for the above market returns. A coin risk assessment can be used to determine the feasibility of the crypto asset, such as if it is possibly a fake coin offering.

6.4 Risks relating to delivery channels.

6.4.1 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 in person, may increase the risk of CASPs being abused by criminals to launder the proceeds of crime. Where an intermediary is used to onboard clients, CASPs 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.

6.4.2 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 their control measures in such terms and conditions to minimise the possibility of the CASPs being abused by criminals.

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

6.5 Geographic risk

6.5.1 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 are less stringent CDD requirements. This, alongside a lack of full implementation of preventive measures, such as the provision of details of the parties to the crypto transaction, as contemplated in Recommendation 16 of the FATF Recommendations (generally known as the "travel rule") and/or the existence of regulatory bodies, creates opportunities that can be exploited by criminal groups. CASPs must take the regulatory requirements in a jurisdiction into account when conducting risk assessment on transactions and clients emanating from such jurisdiction. Enquiring about the implementation of FATF's Recommendation 16

("travel rule") in a jurisdiction may provide an indication of the risk-mitigation factors that have been introduced by such jurisdiction.

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

6.5.3 Similarly, there have been instances of CASPs that have been liquidated as a result of poor governance procedures in some jurisdictions. It is also possible that CASPs in some jurisdictions may have been involved in money laundering to remain viable especially where there have been fluctuations in the crypto asset share price. A possible reason for this is that these CASPs are still emerging, but the sector is seen as having much potential. There have been several cases globally of directors or senior managers of CASPs that have been fined or even sentenced to imprisonment. CASPs should be mindful of adverse media, especially where it involves other CASPs.

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

- That are subject to a travel ban
- Which the FATF regards as being of 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.

6.5.5 The global nature of crypto assets allows for customers that are conducting business and transferring value internationally. This also enables criminals to penetrate the CASP's software and misappropriate crypto assets of other clients. There is further appeal due to foreign and other crypto asset criminals being able to convert their crypto assets into foreign currency of their choice. Therefore, CASPs must have heightened consideration for international crime syndicates, which may not be as

predominant in other sectors. Transactions conducted with clients in jurisdictions known to be susceptible to crime syndicates should be subject to higher scrutiny.

6.6 Terrorist financing risk

6.6.1 In October 2015, FATF released a report entitled *Emerging Terrorism Financing Risks*, which analysed the terrorist financing risks associated with the use of crypto currency. This report highlighted that some crypto currencies 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 organisations to instantly, and largely anonymously, transfer funds worldwide. It also makes it more difficult to implement counter-terrorist financing measures. Crypto assets may be used to finance terrorism. Owing to the decentralisation and anonymity features of crypto currencies, illegal crypto transactions cannot be regulated. The US Federal Reserve, in its 2022 National Terrorist Financing Risk Assessment, has warned that crypto assets may be vulnerable to abuse by terrorist financiers because they can enable anonymous cross-border peer-to-peer funds transfers. The risk assessment also provides information on cases where US law enforcement interfered in terrorist financing activities.

6.6.2 Terrorist organisations may rely on crypto assets for three main reasons.

- Crypto assets are generally characterised by the anonymity of transactions and the largely unencumbered cross-border flow of funds. Hence, terrorists can easily conceal the source and location history of their funds. Terrorists may also find it easy to circumvent foreign exchange quotas and regulations on foreign exchange remittances abroad.
- As the identity of the crypto currency 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 remaining largely unknown.
- The “convertibility” of crypto assets allows terrorists to turn crypto assets into fiat currency. Simultaneously, the decentralised nature of crypto currency assets also provides an opportunity for terrorists to escape banks and other

financial institutions as well as government scrutiny and supervision, enabling them to quickly transfer funds without the knowledge of formal financial institutions.

6.6.3 An emerging trend is where terrorist groups appeal to the public through advertisements (online or in print) to donate to their wallet address directly. This can be in the guise of seeking donations for humanitarian causes in areas of conflict, or for the terrorist groups themselves. The advertisements are often flighted via social media, where the address of their wallet is provided. These appeals sometimes coincide with urgent needs for humanitarian aid in areas where there are terrorist activities.

6.6.4 Information on the use of crypto assets in the financing of terrorism in South Africa is not generally available. The first criminal trial of this nature in the country is currently under way (see “Case Study 2” below). There are, however, international cases that provide information on how crypto transactions were used to obtain funds for terrorist activities.

6.6.5 Crowdfunding campaigns, often disguised as requests for humanitarian aid to war-torn areas, are also used to fund terrorist organisations. Such campaigns vary from highlighting the true plight of victims in these areas (and then using such funds for terrorist financing) to requests that are more explicit in seeking funds for terrorist activities. Crypto currencies are abused by the creation of new crypto addresses in various currencies, resulting in small to large donations being received from a variety of sources.

6.6.6 Although, crypto currencies are not regarded as a widely used method to fund terrorist activities, it is still very important that the public and private sectors co-operate to identify transactions that could potentially end up with terrorist organisations. In such a co-operation model, private sector institutions including CASPs, blockchain analytics and crypto exchanges must be able to provide information on possible terrorist financing activities, while the public sector has a crucial role to play in creating awareness of potential terrorist financing risks.

6.6.7 CASPs must know how to access the referenced targeted financial sanctions (TFS) list, which is available on the FIC website (https://www.fic.gov.za/targeted-financial-sanctions/). CASPs must use this list to 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

6.7.1 The United Nations Security Council (UNSC) has imposed financial sanctions on the Democratic People's Republic of Korea (DPRK) to prevent the country from funding its weapons of mass destruction (WMD) and ballistic missile programmes.

6.7.2 The DPRK has been known to use operators to gain access to CASPs and misappropriate crypto assets of other customers and use money laundering methods to funnel such misappropriated funds to circumvent restrictions.

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

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

7.1 The following could be regarded as ML and 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 crypto assets.
- Sender or recipient profiles – unusual behaviour can suggest criminal activity.
- Lack of ML and 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.
- Crypto assets facilitating 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 CASP at short notice or in a manner that does not make economic sense.
- Crypto assets have many legitimate uses, but they also attract launderers and terrorist financiers because transactions can be anonymous, fast, automated and global in nature, making it difficult and time-consuming for law enforcement agencies to trace the proceeds of the crypto assets being moved.

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

7.2.1 **Irregularities observed during account creation:**

- 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 or 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.

7.2.2 **Irregularities observed during CDD process:**

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

7.2.3 **Profile of potential money mule or scam victims**

- Sender does not appear to be familiar with crypto asset 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 another 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 FATF's Recommendations 15 and 16 aim for effective regulation of CASPs and the crucial interface between crypto assets and fiat currencies. Therefore, AML and CFT standards that apply to traditional financial transactions should, as far as possible, also cover blockchain-based financial services.

8.2 Ultimately, the intention is to bring transparency to crypto transactions. The wire transfer rule (FATF Recommendation 16), also known as the ‘travel rule’, requires jurisdictions to take precautions to ensure that CASPs monitor and share customer data between

each other and make the information available to relevant authorities on request. In this regard, the FIC issued Directive 9 on the implementation of the travel rule for CASPs which enters into operation on 30 April 2025.

8.3 Institutions and individuals in the crypto sector 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 crypto assets are more transparent and accountable compared to fiat currencies. Another aspect is that money laundering using crypto assets is comparatively small in terms of volume, and mainstream media is focusing more on criminal activities related to crypto assets rather than technology and innovation. Albeit on a small scale, there is no doubt that crypto assets are being used to facilitate money laundering and terrorist financing.

8.4 CASPs should ensure they apply robust means of verifying the identity of people who transact with crypto assets. They should be able to match and relate blockchain transactions with true identities, creating an end-to-end trail to assist where there are AML or CFT investigations. Monitoring tools that seek out suspicious transaction patterns for further investigations are also essential for the AML/CFT compliance programmes of crypto assets.

8.5 Cyber criminals use crypto asset to add anonymity to their transactions. But, while crypto assets may provide some advantages over traditional methods of money laundering, the technology is also publicly recorded and accessible, making every transaction traceable. This includes crypto wallets which are publicly available, that were previously used in the commission of crimes. Similarly, there are crypto asset addresses that have been blacklisted by certain regulatory authorities abroad, which are publicly available as well.

8.6 Regulatory measures in South Africa, as applicable to CASPs, are intended to manage and mitigate emergent ML and TF risks facing the sector. These measures include, that CASPs are licensed by FSCA and registered with the FIC, subject to effective monitoring and supervision and are compliant in terms of the FIC Act and standards set by the FATF.

Inherent risk

8.7 Due to the potential for abuse, as explained in paragraph 3.3, the challenges and red flag indicators, the fact that the sector is still relatively new in the regulatory framework and that mitigating supervisory measures are still being refined, the overall inherent risks of money laundering for CASPs in South Africa, based on national and international experience, can be classified as “high”.

8.8 Due to the potential impact of terrorist activities, international experience and investigations of terror financing in South Africa, where crypto assets were used, the inherent TF risk for the sector can also be classified as high.

Residual risk

8.9 As mentioned in paragraph 3.1, the regulatory framework for CASPs in South Africa has been implemented and is functioning effectively. Altogether regulatory obligations imposed upon CASPs have contributed to reduce the residual ML risks of the sector from “high” to “**medium-high**” due to the following developments, and supervisory actions:

(i) The existence of the AML/CFT/CPF regulatory regime applicable to CASPS, who became accountable institutions under designation and registration with the FIC as item 22 of schedule 1 to the FIC Act

(ii) The registration of certain CASPs as an accountable institution under item 12 of Schedule 1 to the FIC Act, following licensing as financial services providers (FSP CASPs) under the FAIS Act

(iii) the supervisory actions by FIC and FSCA including monitoring of registrations, licensing and reporting actions of CASPS,

(iv) the analysis of regulatory reports filed with the FIC by CASPs, and assessment of emerging risks involving CASPs,

(v) risk based supervisory action by FIC and FSCA, including undertaking the risk-based inspections of CASPS,

(vi) the FIC issuance of administrative sanctions on CASPs for non-compliance with FIC Act Directive 7 of 2023.

8.10 Due to the potential impact and national and international experience, the residual risk for TF remains at “high”.

8.11 The sector will continue to be monitored and, the ML and TF risk rating of the sector may be revised in future, if new information becomes available and as the supervision of the sector matures. It is envisaged that an updated sector risk assessment will be undertaken within the next two years.

Ends

Issued by the FIC
1 April 2025

ANNEXURE A

Case study 1:

There are strong informal and small business Bitcoin economies growing in South Africa using decentralised peer-to-peer networks. They use smart contract functionality in the blockchain to enable instant payments across a network of participants via the Lightning Network. This network is a decentralised system for instant, high-volume micro-payments that removes the risk of delegating custody of funds to trusted third parties.

Bitcoin, the world's most widely used and valuable digital asset, allows anyone to send value without a trusted intermediary or depository. Bitcoin contains an advanced scripting system allowing users to programme instructions for funds. There are, however, some drawbacks to Bitcoin's decentralised design. Transactions confirmed on the traditional Bitcoin blockchain take up to one hour before they are irreversible. Transactions on the Lightning Network and peer-to-peer exchanges are immediate.

Micro-payments or payments of a few rand are inconsistently confirmed, and fees render such transactions unviable on other networks. The Lightning Network solves these problems. It is one of the first implementations of a multi-party smart contract (programmable money) using Bitcoin's built-in scripting. The Lightning Network is leading technological development in multiparty financial computations with bitcoin.

These transactions take place through funds that are placed into a two-party, multi-signature "channel" a bitcoin address. This channel is represented as an entry on the bitcoin public ledger. To use funds from the channel, both parties must agree on a new balance. The current balance is stored as the most recent transaction signed by both parties, spending from the channel address. To make a payment, both parties sign a new exit transaction spending from the channel address.

By July 2024, around 11 215 locations worldwide were accepting bitcoins over the Lightning Network. There has lately been an increased number of entities accepting any bitcoin payment methods.

Research shows that 520 businesses in South Africa already transact by using handheld point-of-sale devices that are connected to the Lightning Network. In some instances, staff at these informal and small businesses are paid by their employers in bitcoin via these cashless systems. Therefore, these transactions are not recorded by any accountable institution. This indicates that the Lightning Network is being used for small transactions, which aligns with its intended use.

Spearheaded by a few ambitious initiatives, such as Bitcoin Ekasi, Bitcoin Ubuntu, and Bitcoin Witsand, which has significantly increased the use of crypto assets, the Southern Cape is set to develop into a pioneering hub for decentralised finance in Africa.

Case study 2:

In a case that is currently before the courts, a South African citizen has been accused of contravening the Protection of Constitutional Democracy Against Terrorist and Related Activities Act, 2004 (Act 33 of 2004)**.**

The suspect allegedly bought Bitcoin worth R11 500 through a CASP in November 2017 and on the same day transferred the bitcoin to an organisation describing itself as an independent charity. However, a preliminary investigation revealed that the transfer was in response to an advertisement appealing for funds for weapons, financial aid and other projects assisting the participants in alleged terrorist activities in another country. Furthermore, it was alleged that the non-profit organisation was linked to two other terrorist organisations**.**

The suspect has pleaded not guilty and the case is still ongoing.

Case Study 3

The FIC published the information below as a case study in its 2002/2003 Annual Report, indicating that, already at that stage there were attempts to abuse CASPs fraudulent activities.

Through enhanced due diligence, a crypto exchange remitter reported their client's use of a falsified bank statement to open a crypto account, leading to them placing a transactional hold on the account. In response to the hold, the institution received instruction from an attorney to transfer the remaining account balance of over R1.2 million to an account held by the client. However, misleading bank details had been provided, with the account in question belonging to a third party. This led to the institution refusing the transfer.

The FIC's analysis indicated the client was a suspected money mule, showing that he had used his account to receive multiple payments of more than R12.7 million from various other suspected mules and then externalised more than R11.7 million of the money in crypto currency to an exchange in the Seychelles.

It was concluded that the subject could be a conduit on behalf of a Chinese national using the crypto asset platform to facilitate the externalisation of illicit flow of funds. SARB's Financial Surveillance department was immediately notified, and they issued a directive locking down the R1.2 million being held, pending further investigation.

Case Study 4

The FIC received information that an individual was the victim of fraud whereby the victim was convinced that a company would assist in providing funding for the upgrade of a shopping complex. In order for the funding to be secured the victim had to transfer an amount to a CASP for insurance purposes.

Upon paying the amount to the CASP the victim was assisted to convert the monies to USD Coin. The victim was then instructed to transfer the total amount to another CASP where the monies should have remained as insurance. The victim however realized the monies were no longer available and realized that she was defrauded.

The FIC followed the funds using open-source searches and established that the USD Coin funds were fraudulently transferred to a Non-Custodial Wallet, a Gnosis Protocol v2 Contract and an Anonymous Custodial Wallet. From the Anonymous Custodial Wallet two transfers were made to a CASP based in South Africa. From the CASP transfers were made

to the bank accounts of South African citizens which the FIC identified as being receivers of the original monies paid by the victim.

The FIC assisted in securing the available monies in the South African bank account, however the remaining funds distributed through the Anonymous Custodial Wallet could not be secured due to the anonymity of the wallets.