



FINANCIAL INTELLIGENCE CENTRE

THE 10TH MONEY LAUNDERING AND TERRORISM FINANCING TRENDS REPORT 2024

Contents

- LIST OF TABLES..... ii
- LIST OF CHARTS iii
- LIST OF ACRONYMS iv
- MESSAGE FROM THE DIRECTOR GENERAL 1
- CHAPTER 1: BACKGROUND..... 3**
 - 1.1. OBJECTIVES OF THE REPORT 3
 - 1.2. FUNCTIONS OF THE FINANCIAL INTELLIGENCE CENTRE..... 3
- CHAPTER 2: TRENDS AND CASE STUDIES 8**
 - 2.1. ILLICIT FINANCIAL FLOWS 9
 - 2.2. ILLEGAL MINING AND ILLICIT TRADE BETWEEN EAST AFRICA AND ZAMBIA 12
 - 2.3. ILLICIT TRADE IN WILDLIFE 17
 - 2.4. TERRORIST FINANCING..... 18
 - 2.5. CYBER-ENABLED FINANCIAL CRIMES 18
 - 2.6. CORRUPTION AND MONEY LAUNDERING 26
- CHAPTER 3: SUPERVISION 35**
 - 3.1. SUPERVISION ACTIVITIES..... 35
 - 3.2. AWARENESS AND TRAINING..... 39
- CHAPTER 4: STATISTICS 41**
 - 4.1. SUSPICIOUS TRANSACTION REPORTS..... 42
 - 4.2. CURRENCY TRANSACTION REPORTS 46
 - 4.3. CROSS BORDER CURRENCY DECLARATION REPORTS 48

LIST OF TABLES

Table 1: On-site inspections conducted 2022-2024	35
Table 2: Monitoring activities conducted 2022-2024.....	35
Table 3: Awareness and Education Activities.....	40
Table 4: Compliance officers approved by the Centre.....	40
Table 5: Number of reports received over a period of 3 years	41
Table 6: Reasons for filing STRs.....	43
Table 7: Number of STRs received by type of reporting entities.....	44
Table 8: Intelligence Reports disseminated.....	45
Table 9: Corporate CTRs by province	47
Table 10: Individual CTRs by province	47
Table 11: Cross Border Currency Declaration Reports by value and number	48
Table 12: Inbound and Outbound Traveler Declarations	49
Table 13: Value of Cross Border Currency Declaration Reports Received	49
Table 14: Top 10 nationalities with the highest value of declarations 2024	49
Table 15: Top 10 nationalities with the highest value of declarations 2023	50

LIST OF CHARTS

Chart 1: AML-CFTP value chain	5
Chart 2: Information flow and chain of responsibilities	7
Chart 3: Suspected IFFs	11
Chart 4: Suspected illicit trade between East Africa and Zambia	14
Chart 5: Suspected illegal mining activities	16
Chart 6: Suspected loan fraud and money laundering	20
Chart 7: Suspected cryptocurrency investment fraud	22
Chart 8: Suspected digital transaction fraud	25
Chart 9: Suspected fraud and corruption	28
Chart 10: Suspected fraud and theft of public funds	30
Chart 11: Abuse of Corporate Vehicles for Suspected Public Sector Corruption	33
Chart 12: Compliance Barometer 2024 and 2023	37
Chart 13: Compliance barometer 2023 and 2022	38
Chart 14: STRs received over a 3-year period	42
Chart 15: Number of disseminated cases 2022-2024	45
Chart 16: Number of CTRs received from 2022 to 2024	47
Chart 17: Number of Declarations from 2022 to 2024	48

LIST OF ACRONYMS

AML/CFTP	Anti-Money Laundering/Countering Financing of Terrorism & Proliferation
AML	Anti-Money Laundering
BO	Beneficial Ownership
CBCDR	Cross Border Currency Declaration Report
CTR	Currency Transaction Report
DNFBP	Designated Non-Financial Businesses and Professions
ESAAMLG	Eastern and Southern Africa Anti Money Laundering Group
FATF	Financial Action Task Force
FIC	Financial Intelligence Centre
FUR	Follow Up Report
LEA	Law Enforcement Agency
ML	Money Laundering
ML/TF/PF	Money Laundering / Terrorism Financing / Proliferation Financing
MVTS	Money or Value Transfer Services
PIP	Prominent Influential Person
PF	Proliferation Financing
SDR	Spontaneous Disclosure Report
STR	Suspicious Transaction Report
TF	Terrorism Financing
VASP	Virtual Asset Service Provider

MESSAGE FROM THE DIRECTOR GENERAL

The Financial Intelligence Centre (the "FIC" or the "Centre") remains committed to strengthening Zambia's Anti-Money Laundering/Countering the Financing of Terrorism and Proliferation (AML/CFTP) framework. The Centre's core mandate is to receive, analyse, and disseminate financial intelligence to competent authorities for further investigation and possible prosecution.

The Centre conducts two types of analysis:

- i. Tactical Analysis – Produces intelligence reports for Law Enforcement Agencies (LEAs) and foreign authorities; and
- ii. Strategic Analysis – Results in public typologies, such as the Trends Report, which informs policy and raises awareness among stakeholders.

The Trends Report has evolved into a vital resource for policymakers, reporting entities, academia, and civil society, supporting evidence-based decision making in AML/CFTP.

In 2024, the Financial Action Task Force (FATF) concluded the 4th round of Mutual Evaluations, assessing both technical compliance (legal frameworks) and effectiveness (actual outcomes). FATF's updated methodology emphasizes non-conviction-based forfeiture under Recommendations 4 and 38 to deprive criminals of illicit assets.

In 2024, the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) updated its Mutual Evaluation procedures in order to align with the FATF's revised assessment procedures. Zambia will be evaluated under this new framework in 2027/2028, necessitating strong national preparation to avoid grey listing which may have negative economic and financial effects.

The Southern African Development Community (SADC) Protocol on Finance and Investment recognises the need to fight against illicit financial flows and money laundering. To actualise Annex 12 of the Finance and Investment Protocol, the SADC in the period under review operationalised the SADC AML Committee. The SADC AML Committee held its inaugural meeting from 21st - 23rd February, 2024 in Johannesburg, South Africa at which the Director General of the Financial Intelligence Centre-Zambia, was elected as the first Chairperson for the period 2024 to 2026.

Following Cabinet approval in 2023, Zambia began its 2nd round of the National Risk Assessment (NRA) in 2024, with the FIC designated as the lead coordinator. Progress includes: formation of working groups, development and use of data collection tools, and ongoing data analysis. Completion of the assessment is expected in 2025.

In 2024, the Centre disseminated 951 (2023: 923) intelligence reports to LEAs of which 573 (2023: 450) were disseminated to the Zambia Revenue Authority (ZRA). ZRA made tax assessments worth ZMW 28.90 billion (2023: ZMW1.2 billion) on 326 reports. The ZMW 28.90 billion comprised principal tax, interest and penalties, subject to collection.

Feedback received from other LEAs on disseminated reports indicated that three (3) conviction-based forfeitures and seven (7) non-conviction-based forfeitures were secured, resulting in the forfeiture of assets valued at USD 26.5 million and ZMW 71.5 million held in fixed property and cash. Further, other cases are still under prosecution and investigation.

Most cases handled in 2024 related to suspected illicit financial flows (IFFs) involving commercial activities such as mispricing of goods and services, mis-invoicing and tax evasion. Further, these disseminations related to money laundering and fraud. The FIC observed that IFFs were mostly enabled by shell companies controlled by foreign nationals. High-risk sectors included retail, wholesale, and mining. Further, the FIC noted a reduction in analysed reports relating to public sector corruption, hence the low number of disseminations on corruption compared to cases relating to money laundering, fraud and tax evasion.

During the period under review, the FIC noted a number of cases involving cyber fraud and regulatory evasion. A number of entities were incorporated under the pretext of providing management consultancy and online learning when in fact the entities were fraudulently dealing in payment system settlement. The Centre noted that prepaid branded cards were being used to illegally move funds in and outside Zambia.

The Money Value Transfer Service (MVTs) Providers experienced unusually high funds transfers particularly in the mobile money agent wallets. Due to their commercial nature, mobile money agent wallets offer higher holding and transaction limits compared to personal wallets. However, due to simplified Customer Due Diligence (CDD) measures existing in the MVTs sector, mobile wallets have become attractive for illicit activities. Simplified CDD measures entail collecting basic identification information when onboarding customers or conducting transactions. MVTs create transaction layers that conceal the true origin of the funds, allowing for laundering and other financial crimes without suspicion. Further, verification of the intelligence established that some mobile money wallets were used for cross border transactions.

I wish to extend my gratitude for the invaluable support that the Centre received from Government through the Ministry of Finance and National Planning. In addition, I wish to thank the Board of Directors for providing effective oversight on the operations of the Centre. I also wish to thank competent authorities, reporting entities and cooperating partners for the support extended to the Centre. Lastly, I wish to thank Management and Staff of the Centre for their outstanding performance in 2024.

The Centre remains steadfast in carrying out its mandate with the Government's ongoing support and cooperation from stakeholders.



Clement K. Kapalu
DIRECTOR GENERAL
FINANCIAL INTELLIGENCE CENTRE

1.1. OBJECTIVES OF THE REPORT

The Trends Report is issued pursuant to Section 5(2)(d) and (f) of the Financial Intelligence Centre Act No. 46 of 2010 (the FIC Act) with the following objectives:

i. Awareness

To provide awareness by educating reporting entities and the general public on their obligations and informing them of measures to detect, prevent and deter ML/TF/PF or any other serious offences relating to ML/TF/PF.

ii. Policy Formulation

To inform government policy formulation based on observed trends and patterns relating to ML/TF/PF and other financial crimes.

iii. Supervision

To undertake effective risk-based supervision and enforcement of AML/CFTP to ensure compliance by reporting entities with the FIC Act.

1.2. FUNCTIONS OF THE FINANCIAL INTELLIGENCE CENTRE

The functions of the FIC as provided under section 5 of the FIC Act are to inter alia:

i. Strategic Analysis

Conduct strategic analysis to identify trends, patterns and any other serious offences relating to ML/TF/PF. One of the products of strategic analysis is typology reports such as the Trends Report.

ii. Tactical Analysis

Receive, request, analyse and evaluate STRs to identify specific targets and follow the trail of particular transactions to determine the links between those targets and possible assets. The product of this process generates financial intelligence that is disseminated to LEAs and foreign competent authorities.

iii. Dissemination

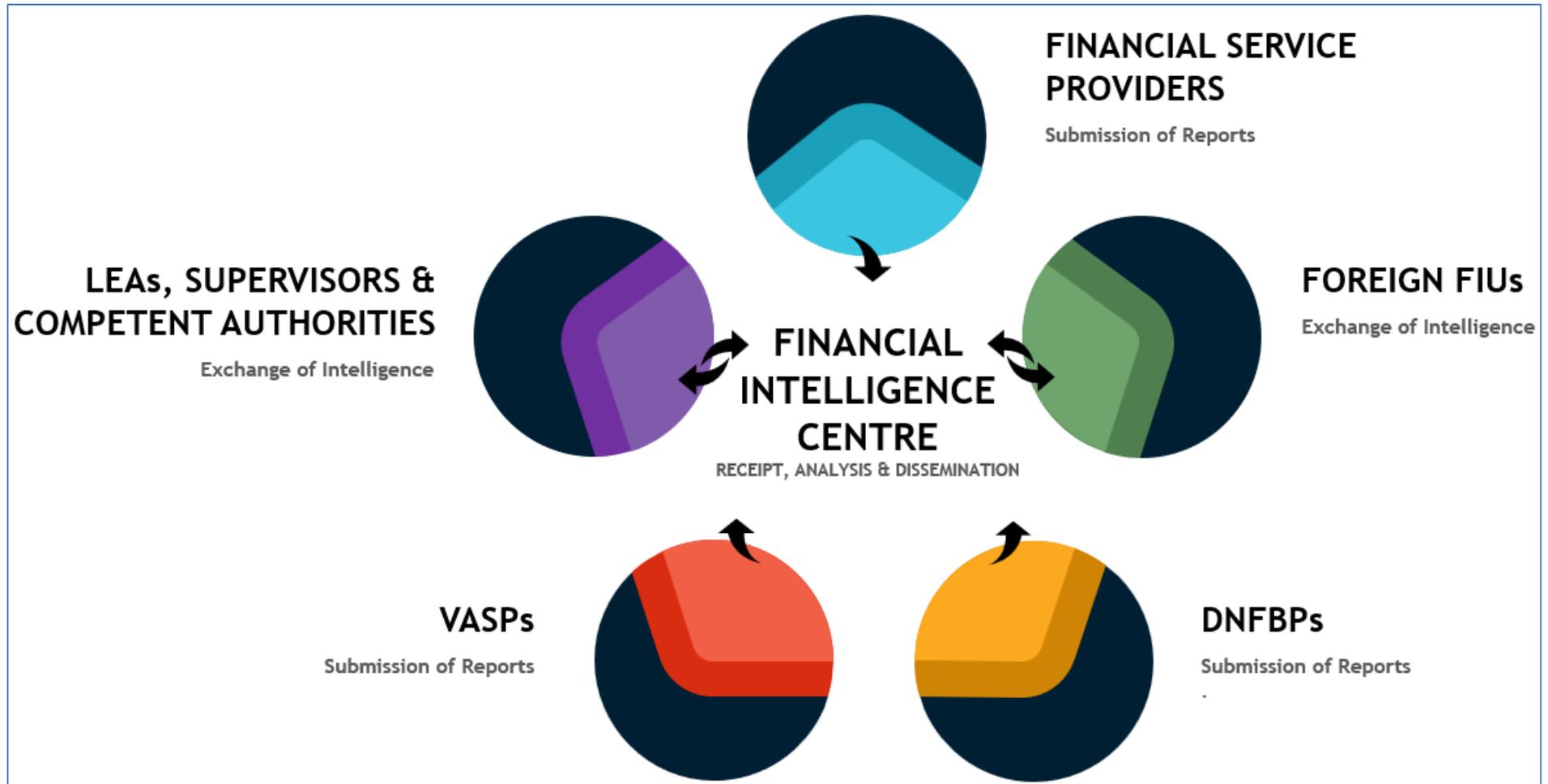
Disseminate information, spontaneously or on request, to LEAs and other competent authorities, where there are reasonable grounds to suspect ML/TF/PF and other financial crimes.

iv. Spontaneous Disclosure

Provide information relating to suspicious transactions to any designated local or foreign authority, subject to conditions that the Director General may determine, in accordance with the FIC Act.

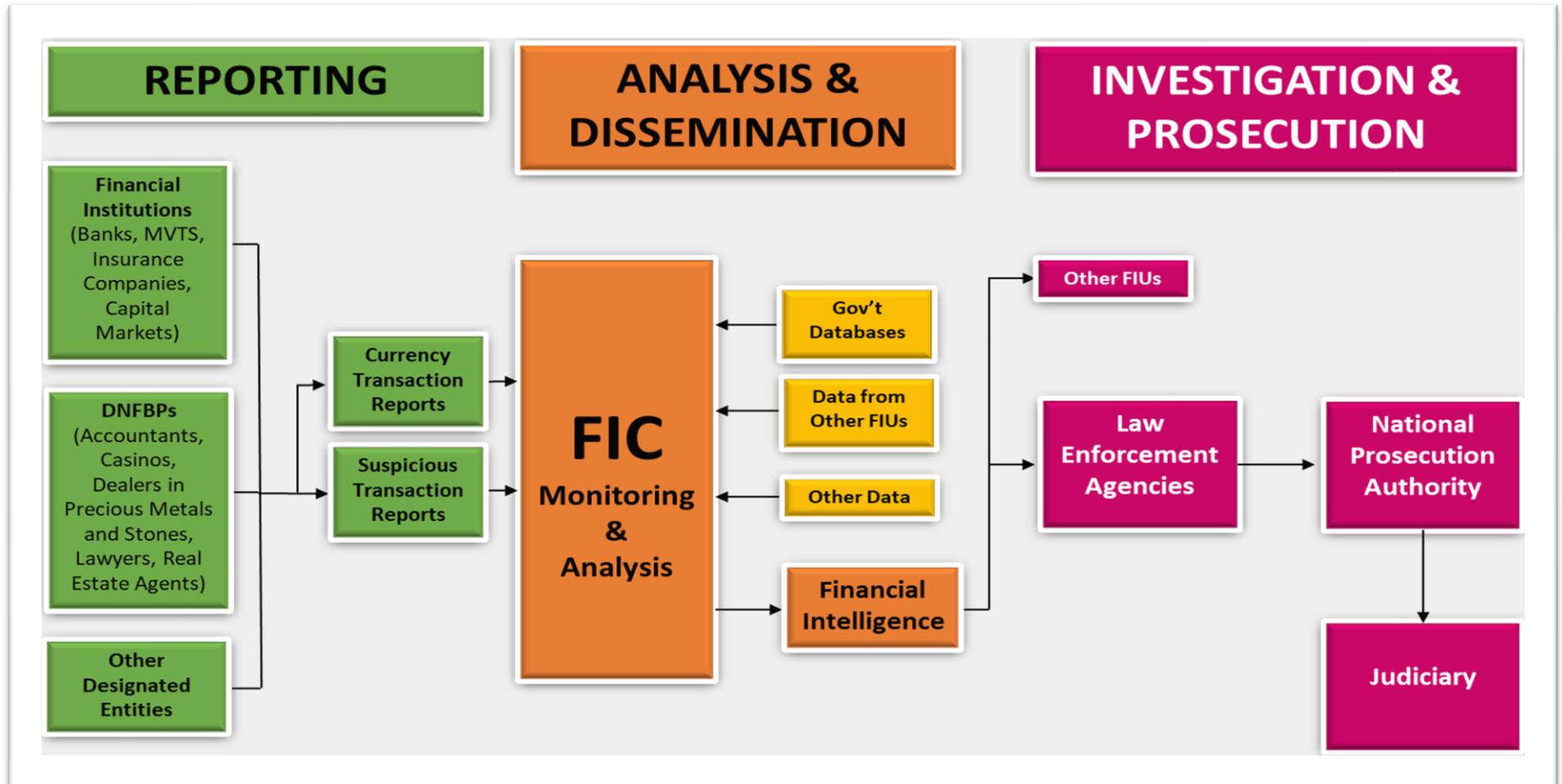
Chart 1: AML/CFTP value chain below demonstrates how the FIC as the national agency interacts with stakeholders in its operation.

Chart 1: AML-CFTP value chain



The FIC receives information from various sources including banks, insurance companies, capital markets, casinos, lawyers, accountants, real estate agents, dealers in precious stones and metals, virtual asset service providers and the public. Upon analysis of this information, financial intelligence is generated, which is disseminated to competent authorities for investigations and possible prosecution where there are reasonable grounds to suspect that crime has been committed. Chart 2: Information flow and chain of responsibilities below shows information flow and chain of responsibilities.

Chart 2: Information flow and chain of responsibilities



During the period under review, the Centre noted continuing and emerging trends in financial crimes in the country. This section discusses continuing and emerging trends along with case studies.

Continuing trends were mostly observed in the following areas: IFFs, money laundering, use of cash in illicit transactions, cyber enabled financial crimes, masking beneficial ownership of corporate vehicles and misuse of corporate vehicles. Emerging trends were observed in illicit mining activities.

Other trends included cyber-enabled financial crimes, environmental crimes including illicit trade in wildlife and mining and public sector corruption. The main methods applied to launder funds from the above-mentioned crimes were the use of cash to hide the audit trail, use of shell companies and concealment of beneficial ownership of corporate vehicles. The identified destinations of the IFFs were mainly Asia, Middle East and South America.

PRIVATE SECTOR MONEY LAUNDERING

During the period under review, the Centre disseminated 872 financial intelligence reports relating to IFFs mostly involving commercial activities. The nature of suspicions in the analysed reports mainly bordered on:

- i. Unusual or complex transactions;
- ii. Suspicious customer behavior;
- iii. Transactions inconsistent with customer profile;
- iv. Use of Zambian owned company and personal accounts to conceal beneficial ownership;
- v. Structured deposits below the reporting thresholds;
- vi. Unusually high USD-denominated cash deposits; and
- vii. Immediate international remittance following cumulation of funds.

The Centre upon analysis of the STRs noted the following trends:

- i. Most of the companies used to move funds were recently incorporated with little or no identifiable corresponding commercial activity;
- ii. Use of forged supporting documentation for outward remittances;
- iii. Purported outward remittances did not have corresponding imports;
- iv. Illegally established smelters are buying minerals from illegal miners. The illegally established smelters in turn sell to legally established mining companies and are paid in foreign currency;
- v. Some of the cash deposits were determined to originate from illicit

- trade in wildlife; and
- vi. Cross border smuggling of locally manufactured goods and currency.

2.1. ILLICIT FINANCIAL FLOWS

IFFs refer to illegal movements of money or assets across borders. These flows often stem from activities such as tax evasion, corruption, illicit trade and financing of terrorism.

The effects of IFFs on the economy include:

- i. loss of both local and foreign direct investment;
- ii. reduced government revenue leading to insufficient funding for healthcare, education and other social amenities;
- iii. undermined governance and weakened rule of law;
- iv. weakened national economy by depleting foreign reserves and distortion of exchange rate regimes;
- v. increased poverty levels especially in the lower income population;
- vi. encourages criminal activity including organized crime and corruption; and
- vii. environmental degradation resulting from illegal mining and logging.

During the period under review, the Centre detected suspected IFFs worth **USD 3.5 billion**. IFFs detected in 2024 were mostly associated with commercial activities perpetuated by multinational enterprises (private sector). A smaller portion was perpetuated by criminal networks and corrupt activities. The number of subjects involved in the illicit transfer of funds was 1,203 which comprised 401 corporates and 802 natural persons. Most of the corporates identified were recently incorporated and did not appear to have any commercial activity to warrant the volume of transactions on their accounts. The natural persons involved were largely foreign nationals. They either transacted on their own accounts or used Zambians to carry out the transactions. These Zambians were either business partners, employees, or simply agents who were remunerated with a commission for their facilitation.

The illegal trade in mining is mainly in the North Western, Copperbelt, Luapula and Muchinga provinces. The minerals illegally traded included copper, gold and precious stones.

Case Study I: Illicit Financial Flows

The FIC analysed STRs linked to a syndicate involving both foreign and Zambian nationals, who collectively incorporated 13 companies using the same business address within the year 2023. The companies were purported to have been dealing in non-specialized wholesale trade. While the company registration documents listed Zambian nationals as the beneficial owners, it was established that the operational control and management of the company accounts was largely dominated by foreign nationals. It was established that many of the Zambian nationals had no known sources of income and lacked active bank accounts, raising suspicion regarding their ownership of the companies.

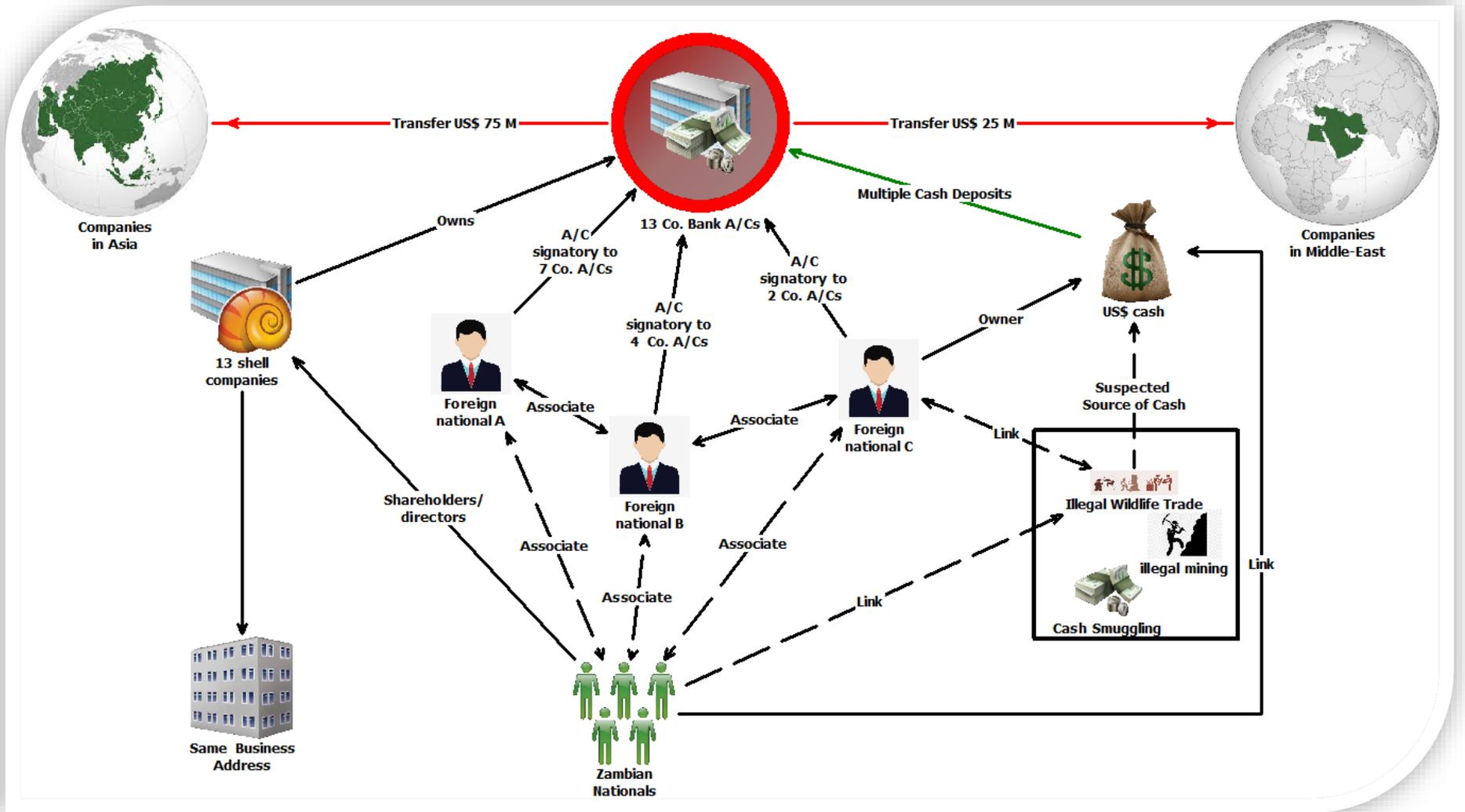
During analysis, **Foreign National A** was identified as the sole signatory on seven company accounts, **Foreign National B** held signatory authority to four accounts, and **Foreign National C** was the signatory to the two accounts. Financial analysis of the company accounts revealed a clear transactional pattern, characterised by multiple third-party cash deposits, each ranging between **USD 75,000** and **USD 100,000**. These deposits were followed by a series of inter-company transfers, ultimately culminating in remittances to foreign jurisdictions, often under the narratives "Payment for Furniture" and "Payment for Goods." The analysis revealed that more than **USD 100 million** had been transferred out of the country to Middle East and Asia by the 13 companies. The suspected economic activities of these companies included illegal mining, cross border currency smuggling and illegal wildlife trade. It was established that the companies were not tax compliant.

Further, the FIC received intelligence from a foreign counterpart, which revealed that the same group of foreign nationals had also established identical companies in that jurisdiction, suggesting a coordinated effort to facilitate large-scale illicit financial activities across borders. The case was disseminated to competent authorities on suspected tax evasion, fraud and money laundering.

The case was under investigations.

Chart 3 below illustrates illicit financial flows.

Chart 3: Suspected IFFs



Recommendations on Illicit Financial Flows:

- i. Government to set limits on the amount of cash that can be used for transactions. This can improve transparency of transactions in commerce;
- ii. Enhance identification and verification of beneficial ownership information of legal persons and arrangements to ensure completeness and accuracy;
- iii. Foster collaboration between countries to share information and resources in combating IFFs;
- iv. Capacitate law enforcement and other competent authorities to detect and investigate IFFs effectively;
- v. Improve monitoring of trade data and electronic payments transactions to facilitate early detection of IFFs; and
- vi. Strengthen the legal and institutional framework on cross border transportation of cash and bullion.

2.2. ILLEGAL MINING AND ILLICIT TRADE BETWEEN EAST AFRICA AND ZAMBIA

During the period under review, the Centre noted an increasing trend of illegal business activities between East Africa and Zambia to facilitate the illegal movement of goods such as grain, timber, minerals among other products. The Centre also observed an increasing trend of illicit mining activities on the Copperbelt.

Case Study II: Suspected Illicit trade between East Africa and Zambia

The Centre analysed a number of STRs involving suspected illegal trade between Zambians and **Country O** nationals based in East Africa. Analysis revealed that the trade often involved nationals of **Country O** bringing into Zambia undeclared currency. This undeclared currency is used to buy minerals which are smuggled back to **Country O** thus circumventing customs regulations and taxes.

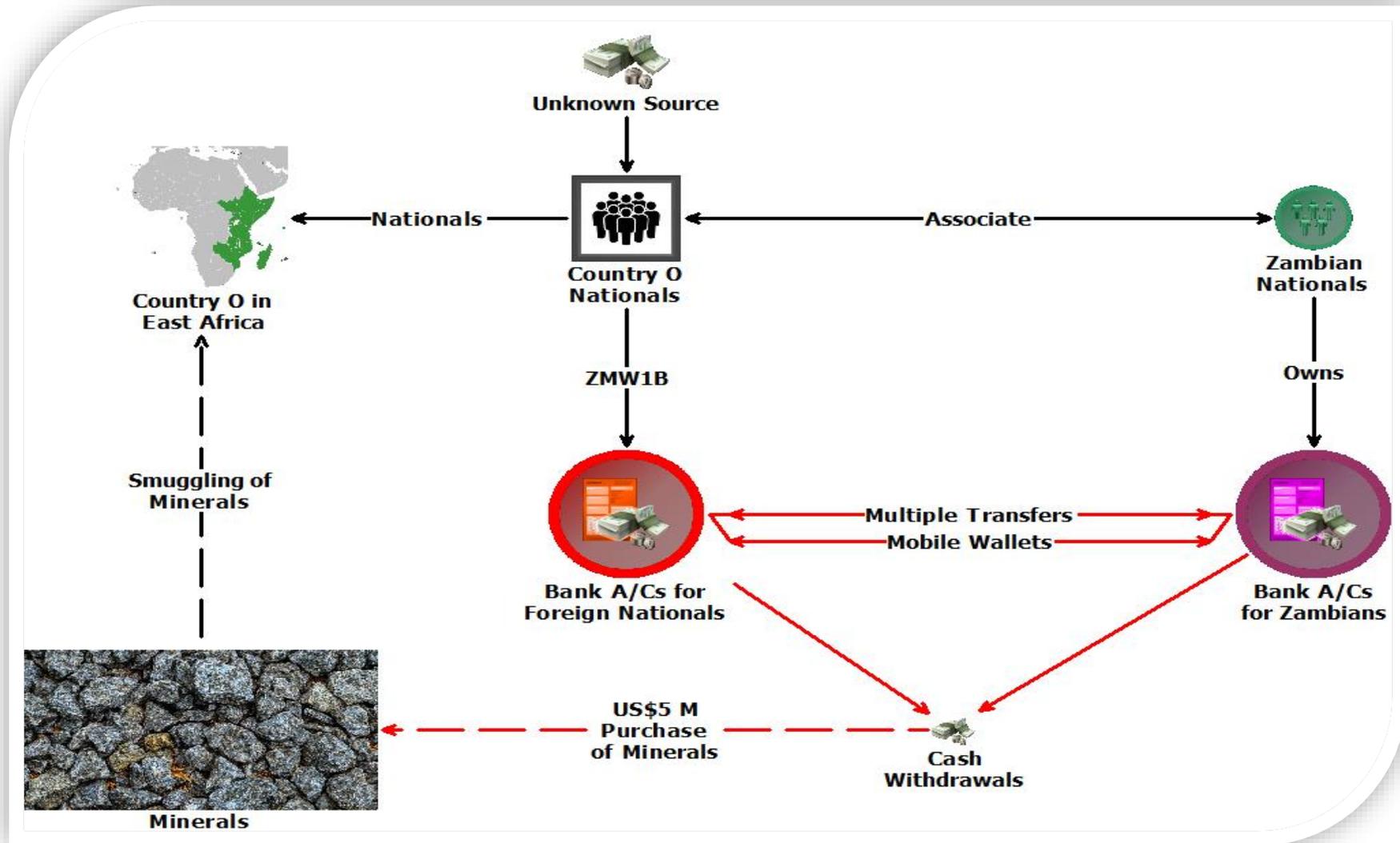
When the undeclared funds are in Zambia, the foreigners open bank accounts and mobile wallets to facilitate the storage and movement of value. Some of these undeclared funds are deposited in bank accounts and mobile wallets belonging to Zambians for the same purpose. These funds are then withdrawn and used to buy illegally mined minerals in districts such as Kasempa, Mufulira, Kitwe, and Chingola. For the period between 2022 and 2024, the subjects bank accounts recorded a total credit turnover of **ZMW 1 billion** and **USD 5 million**.

It was noted that this illicit activity thrived due to the porous border between Zambia and **Country O** and the ease with which foreign nationals are able to open bank accounts and mobile wallets in Zambia.

The case was disseminated to LEAs for possible tax evasion and money laundering. The case was under investigations.

Chart 4 below illustrates suspected illicit trade between East Africa and Zambia.

Chart 4: Suspected illicit trade between East Africa and Zambia



Case Study III: Suspected Illicit Mining Activities

The Centre analysed reports of suspected illicit mining activities on the Copperbelt Province. The analysis revealed that **Individual X** and associates (Asian nationals) incorporated **Company Y** in 2020. **Company Y** was registered for wholesale trade but the transactional activity appeared suspicious.

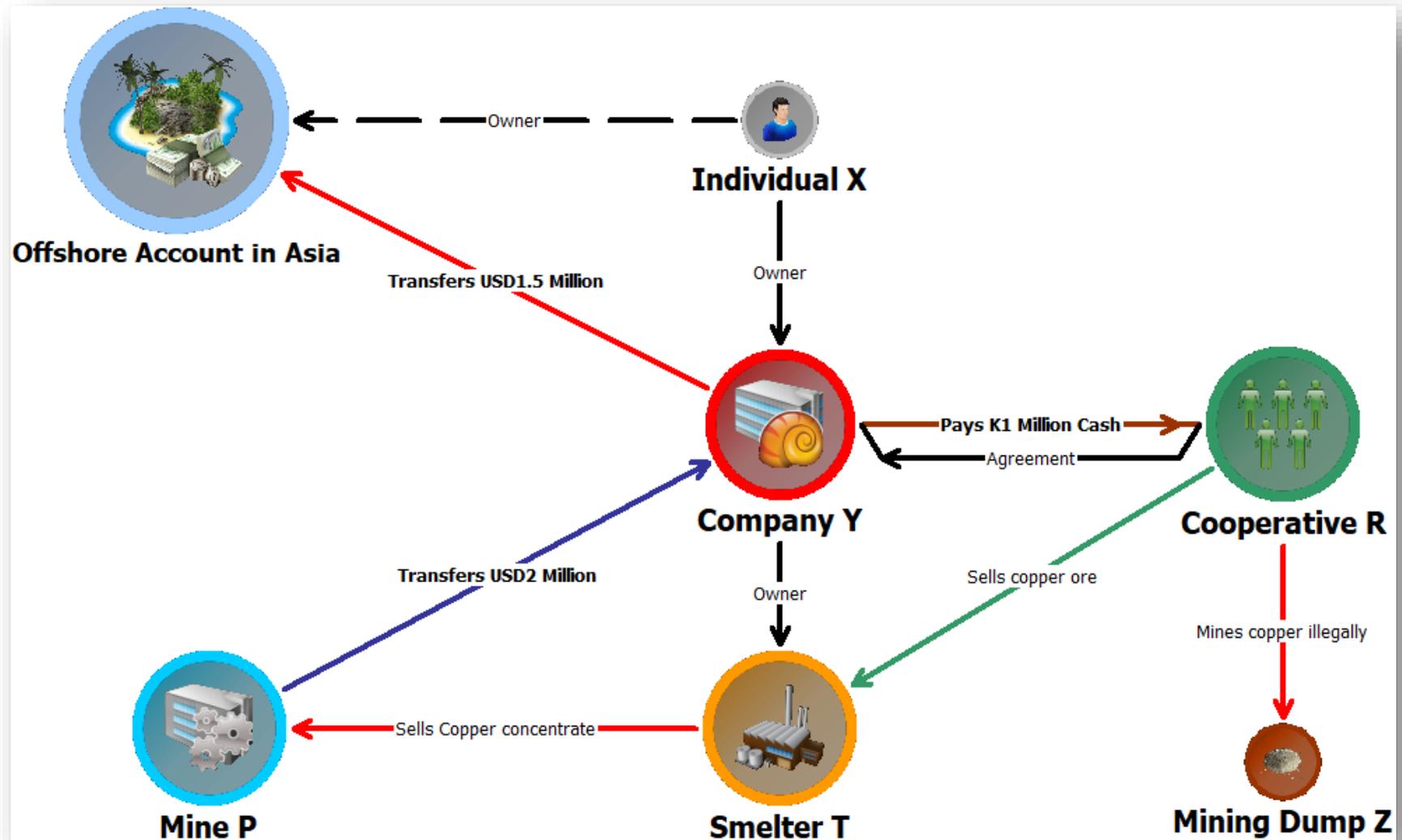
Analysis revealed that **Company Y** was in an agreement with **Cooperative R** that was mining copper ore from a mining dump **Z**. It was established that **Cooperative R** was owned by Zambian nationals and did not possess permits to mine copper ore. The extracted copper ore was sold to **Company Y** which owns an illegal smelter called smelter **T**. **Company Y** paid **Cooperative R** ZMW 1 million in cash for the extracted copper ore to avoid detection.

Company Y through **Smelter T** then sold the copper concentrate to **Mine P**, an established mining firm operating in Zambia. Analysis of the bank statements revealed that **Company Y** had received in excess of USD 2 million from **Mine P**. **Company Y** was observed to have externalised the funds in excess of USD 1.5 million to offshore accounts in Asia.

The case was disseminated to LEAs on suspected tax evasion and money laundering. The case was under investigations.

Chart 5 below illustrates suspected illegal mining activities.

Chart 5: Suspected illegal mining activities



Recommendations on illegal mining and illicit trade between East Africa and Zambia:

- i. Reporting entities to comply with requirements of the FIC Act on opening accounts for non-resident clients.
- ii. Strengthen KYC measures related to non-resident customers.
- iii. Government to enhance detection of the movement of cash and bullion at entry and exit points of the country; and
- iv. Government should strengthen the monitoring of small-scale miners, ensuring that they operate with the necessary permits and conduct business with regulated mining firms.

2.3. ILLICIT TRADE IN WILDLIFE

During the period under review, the Centre analysed a case bordering on suspected wildlife crime involving Zambian nationals and foreign nationals working together to illegally harvest and transport Mopane logs.

Case study IV: Suspected Wildlife Crimes

The Centre analysed a spontaneous disclosure report on four trucks intercepted in **Town A** carrying suspected illegal logs intended to be exported to **Country M** through border **Y** without the necessary permits. The report indicated that when the trucks were intercepted, **6 foreign nationals** were arrested. Further, the LEAs arrested and charged Individual **N** who was a Director/Shareholder in **Company ZZ**, a foreign owned company, for attempting to export forest produce without an export permit, an offence under the Forest Act No. 4 of 2015.

One of the trucks seized contained **sixty-five (65)** Mopane logs, which were allegedly loaded at a warehouse owned by **Company ZZ**. It was further reported that a search conducted by LEAs at the premises of **Company ZZ** led to the seizure of properties.

The analysis revealed that **Company ZZ** was receiving funds from **Companies DA, RS** and **CS** based in Asia, that were in the business of selling furniture and other timber products. The funds transferred by these companies were believed to have been payments for the mopane logs illegally exported by **Company ZZ**. Further analysis established that **Companies DA, RS** and **CS** transferred **USD 210,000, USD 91,000** and **USD 12,000** respectively to **Company ZZ** in 2024.

The case was disseminated to the appropriate LEAs on corruption, wildlife crime and money laundering. The matter was under investigations. Recommendations on Illicit Trade in Wildlife:

- i. Capacitate competent authorities responsible for the management, harvesting, transportation and export of forestry resources with adequate personnel and modern technology to monitor illegal wildlife trade by,
 - a) Deploying monitoring and enforcement technologies such as remote sensing and satellite imagery and using drones for patrols. Smart mobile communications tools with GPS tracking and realtime reporting.
 - b) Increasing the number of skilled personnel.

2.4. TERRORIST FINANCING

During the period under review, the Centre analysed a case bordering on suspected Terrorist Financing.

Case Study V Suspected Terrorism Financing

The FIC analysed a suspicious transaction report relating to an individual **S**, purporting to be a Zambian national. The report alleged that **Individual S** matched the identity of **Individual O**, a foreign national on the United Nations Sanctions List, as a person who was charged for terrorism financing activities. The subject was believed to be facilitating the movement of funds and recruitment of persons for various suspected Terrorist groups in the Southern African region. The analysis established that **Individual S's** identity details were that of **Individual O**, the individual involved in terrorism financing activities. The subject is suspected to have changed the name from **O** to **S** in order to elude law enforcement authorities. Analysis established that **Individual S** had opened a bank account in Zambia. The bank account transactional activity was characterised by low value cash deposits and transfers to several mobile money wallets. The bank account was closed due to inactivity.

The case was disseminated to the relevant competent authorities for investigations.

Recommendation on Terrorist Financing:

- i. Government to finalize the project on the integrated national registration information system which would reduce the falsification of identification documents; and
- ii. Enhance information exchange mechanisms both domestically and regionally on terrorist financing.

2.5. CYBER-ENABLED FINANCIAL CRIMES

The Centre has noted that the financial services industry is the target of a growing number of cyber-enabled financial crimes in Zambia. It has been

noted that most of the financial crimes in the cyberspace have been committed by East Africans collaborating with Zambian citizens. Increased automation and dependence on electronic payment systems has contributed to an increase in cyber-enabled financial crimes.

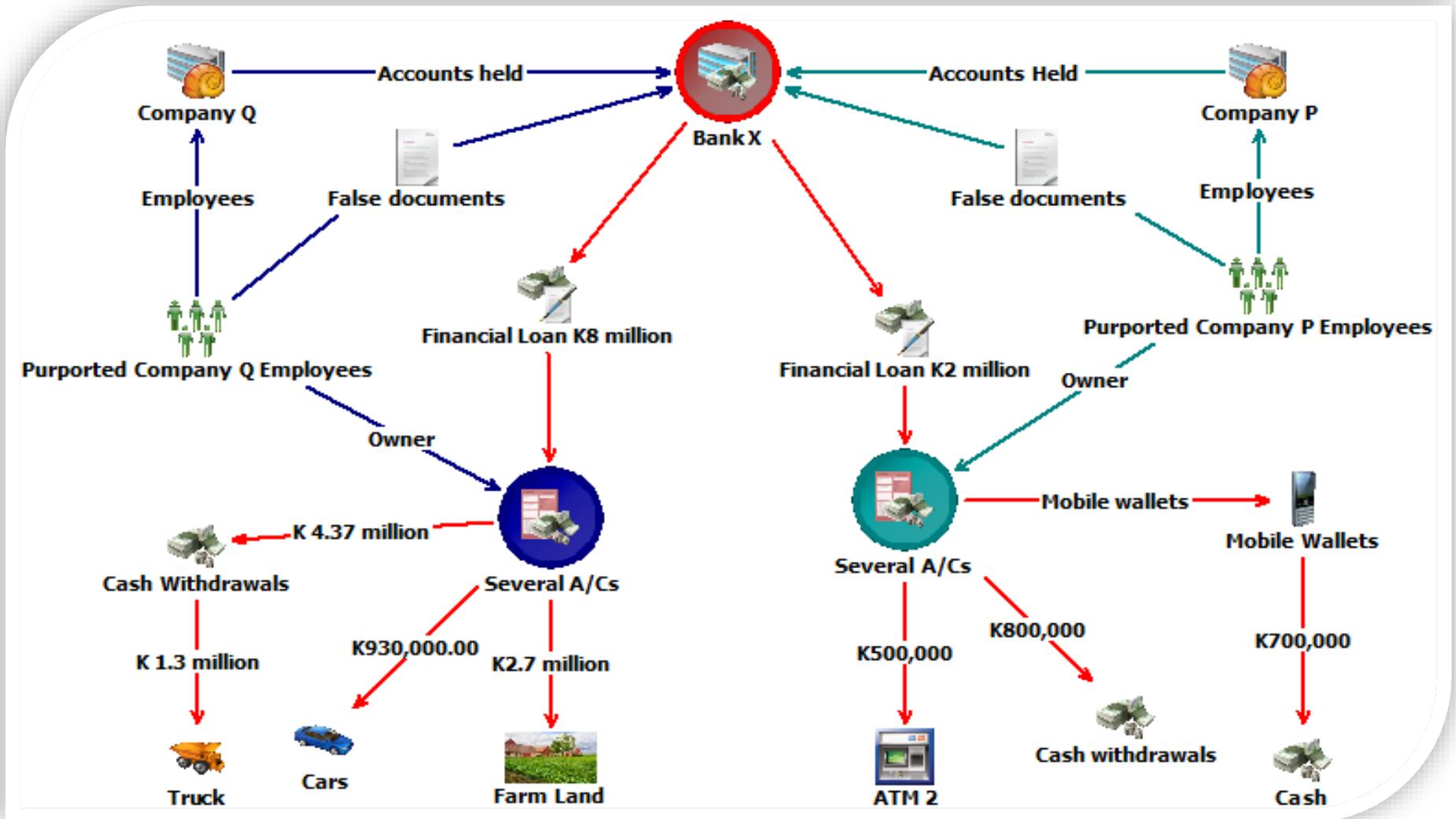
Case Study VI: Suspected Loan Fraud and Money Laundering

The FIC analysed STRs involving suspected fraud regarding a loan obtained from **bank X**. Our analysis revealed that 25 individuals purported to be employees of **Company Q** and **Company P** respectively were suspected to have colluded with the company directors to defraud the bank through a loan scheme facility. Verification revealed that **Company Q** and **Company P** were shell companies. A review of bank statements for the 25 individuals revealed that they received loans valued at **ZMW 10 million**. Further analysis revealed that most of the funds were obtained through cash withdrawals, ATMs, mobile money and used for the purchase of luxury cars, heavy-duty motor vehicles, farm land and equipment.

The matter was disseminated to the relevant LEA and was under active investigation.

Chart 6 below illustrates suspected loan fraud and money laundering.

Chart 6: Suspected loan fraud and money laundering



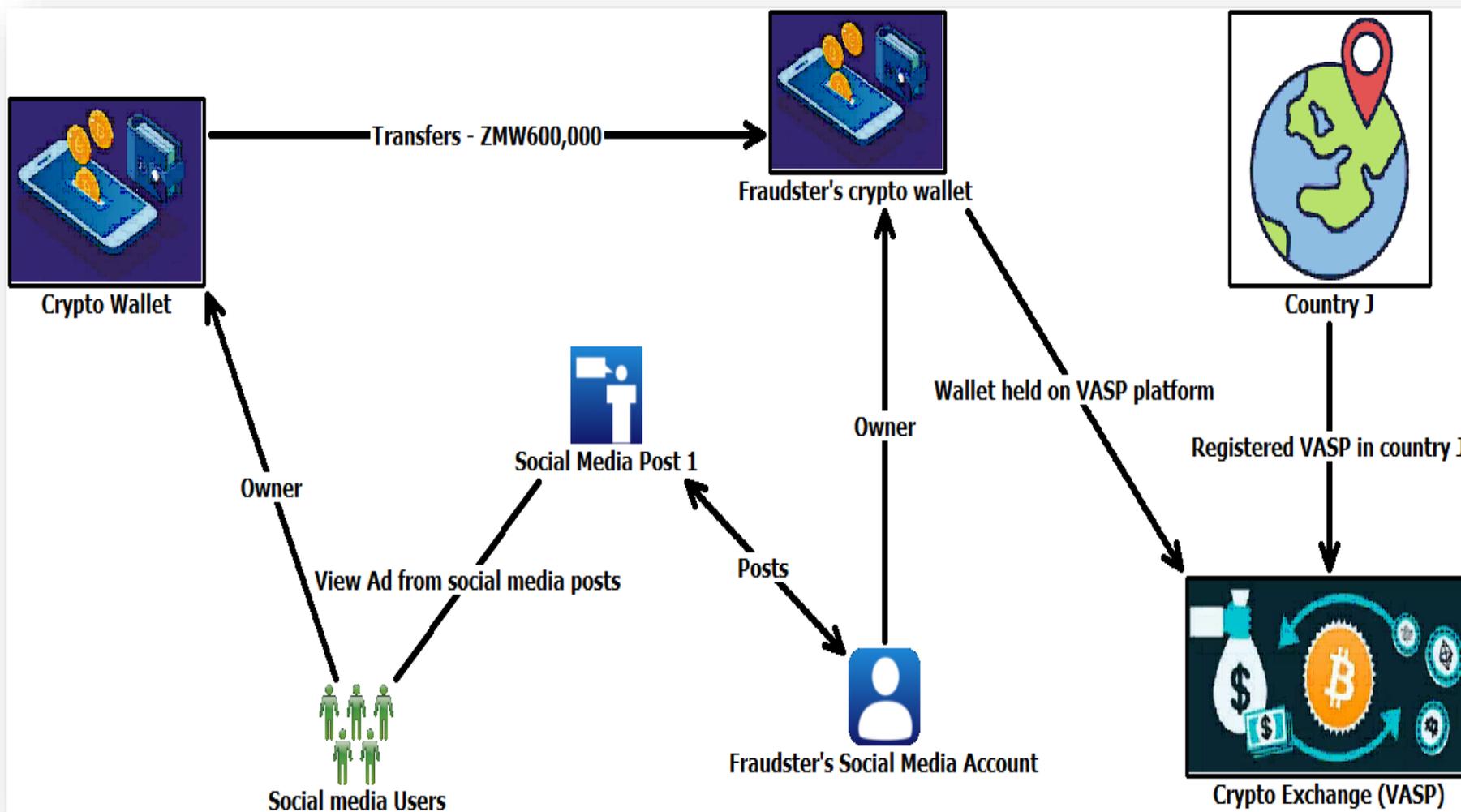
Case Study VII: Suspected Cryptocurrency Investment fraud

The FIC analysed a case following receipt of multiple transaction reports of suspected investment fraud involving Zambian nationals who were defrauded through accounts held at a crypto exchange site in **Country J**.

It was established that the Zambian nationals were lured into making investment in cryptocurrency by unknown individuals through social media. The wallet addresses the funds were remitted to were not registered with their Virtual Asset Service Provider (VASP) but another VASP registered in **Country J**. The subjects received neither interest on their investments nor their principal investment. It was determined that the wallet accounts which received the funds had withdrawn a portion of them through a VASP registered in **Country J**. The victims invested approximately **ZMW 600,000** over a period of 6 months.

The matter was disseminated to the relevant LEA and was under active investigation. Chart 7 below illustrates suspected cryptocurrency investment fraud.

Chart 7: Suspected cryptocurrency investment fraud



Case Study VIII: Suspected Cyber Fraud

The FIC analysed a suspicious transaction report on suspected cyber fraud involving **Company Q**. It was established that **Company Q** was using their Point of Sale (POS) machines to initiate fraudulent transactions on credit and debit cards of various individuals. **Company Q's** POS service provider was contacted by various individuals claiming that their cards had been used on their payment system without their knowledge. Verification of the card details belonging to some of the complainants showed that indeed their cards had been used to make payments on POS machines for **Company Q**. A review of the payment system activities showed that **Company Q** conducted transactions worth over **ZMW 2 million** using multiple cards over a period of one week. Further, several other transactions involving different card numbers were identified as unusual.

The case was disseminated to the relevant LEA on suspected fraud. The case remains under investigations.

Case Study IX: Suspected Digital transaction fraud

The FIC analysed STRs on **Company B** and **Company A**. It was alleged that the two (2) companies' bank account credit turnovers exceeded the annual expected declared income and the source of funds could not be traced. Further, it was alleged that **Company B's** account was dealing in Crypto currency. Analysis conducted revealed that **Company B**, a company incorporated in **Country Y** in East Africa held an account in Zambia with **Bank Z** and was using the account to receive fund transfers from Zambian incorporated companies, **Company A** and **Company C**. **Company B's** bank account credit turnover for a period of five months was in excess of **USD30 million**. Further, the credit turnover for **company A** and **company C** was **USD10 million** and **USD2.8 million**, respectively. All the entities accounts were opened under the pretext of management consultancy and online learning when in fact, the entities were dealing in suspected fraudulent payment system settlements from processing prepaid Master and Visa cards from questionable sites located outside Africa.

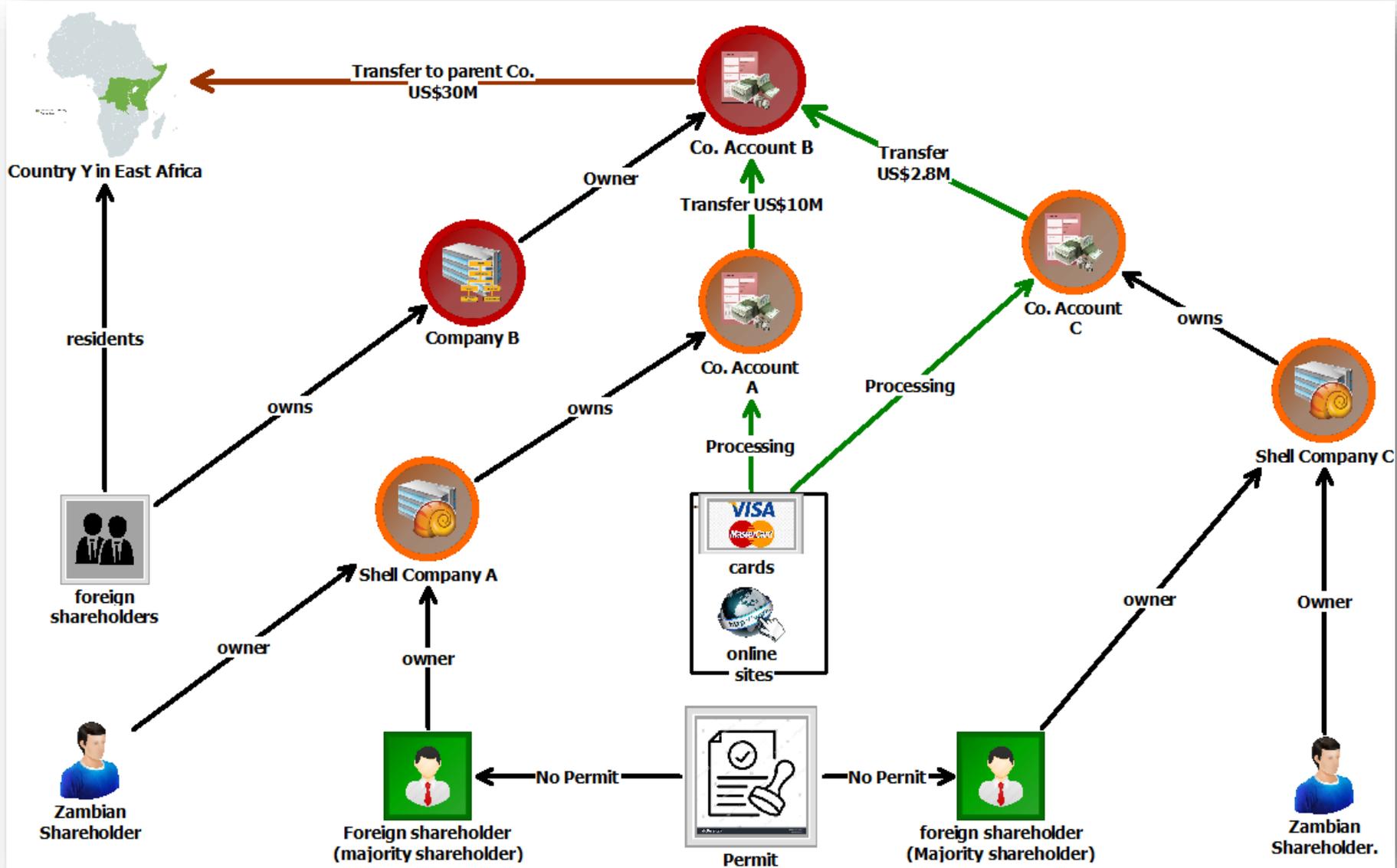
Further, verifications conducted with the regulator on the status of **Company A** and **Company C** revealed that they were not registered to engage in payment settlement transactions, were not registered for any taxes in Zambia and the listed foreign beneficial owners of the entities did not possess any permits to operate businesses in Zambia. The source of funds observed which were credited to the company accounts mostly through fund transfers raised suspicion of the possibility of the companies being involved in illicit financial

activities. The findings suggest that **Company A** and **Company C** are shell companies established to facilitate money laundering activities, disguising their operations as financial and management consultancy as well as online learning.

The case was disseminated to competent authorities on suspected fraud, money laundering and tax evasion. The case was under investigations.

Chart 8 below illustrates suspected digital transaction fraud.

Chart 8: Suspected digital transaction fraud



Recommendations on cyber enabled fraud:

- i. Financial institutions must enforce stringent Know Your Customer (KYC) and enhanced due diligence (EDD) measures to verify the legitimacy of entities and transactions especially for accounts held by non-residents;
- ii. Financial institutions should enforce strict Know Your Employee (KYE) measures to avoid the abuse by employees to facilitate illicit financial activities;
- iii. Financial institutions must adhere to their obligations to file STRs within the stipulated timelines;
- iv. Financial institutions should tighten internal controls related to lending; and
- v. Public awareness programmes by service providers and supervisory authorities to sensitise the public on virtual asset activities or operations.

PUBLIC SECTOR CORRUPTION AND MONEY LAUNDERING

2.6. CORRUPTION AND MONEY LAUNDERING

The Centre analysed cases related to suspected public sector corruption and money laundering. The Centre noted a reduction in analysed reports relating to public sector corruption from 55 in 2023 to 40 in 2024 as depicted in table 6. The cases bordered on suspected abuse of authority of office and corruption.

The methods associated with public sector corruption included:

- i. Non-delivery of contract obligation;
- ii. Facilitation payments; and
- iii. Fraudulent payments.

Case Study X: Suspected Fraud

The FIC analysed a spontaneous disclosure report of suspected misclassification of an import by **Company K**. The disputed misclassification between **Company K** and public **Institution Y** was adjudicated in the courts of law and the matter was decided in favour of **Company K**. **Company K** was awarded USD 15 million. However, the parties agreed to a reduced amount of USD 10 million.

Institution Y made an initial 50% payment of USD 5 million to **Company K** based on the agreed amount. **Individuals X** and **Q**, then employees of Institution Y, fraudulently facilitated the payment of the outstanding balance of USD 5 million to **Company J's** account held at **Bank Z**. **Company J** is owned by **W, T**

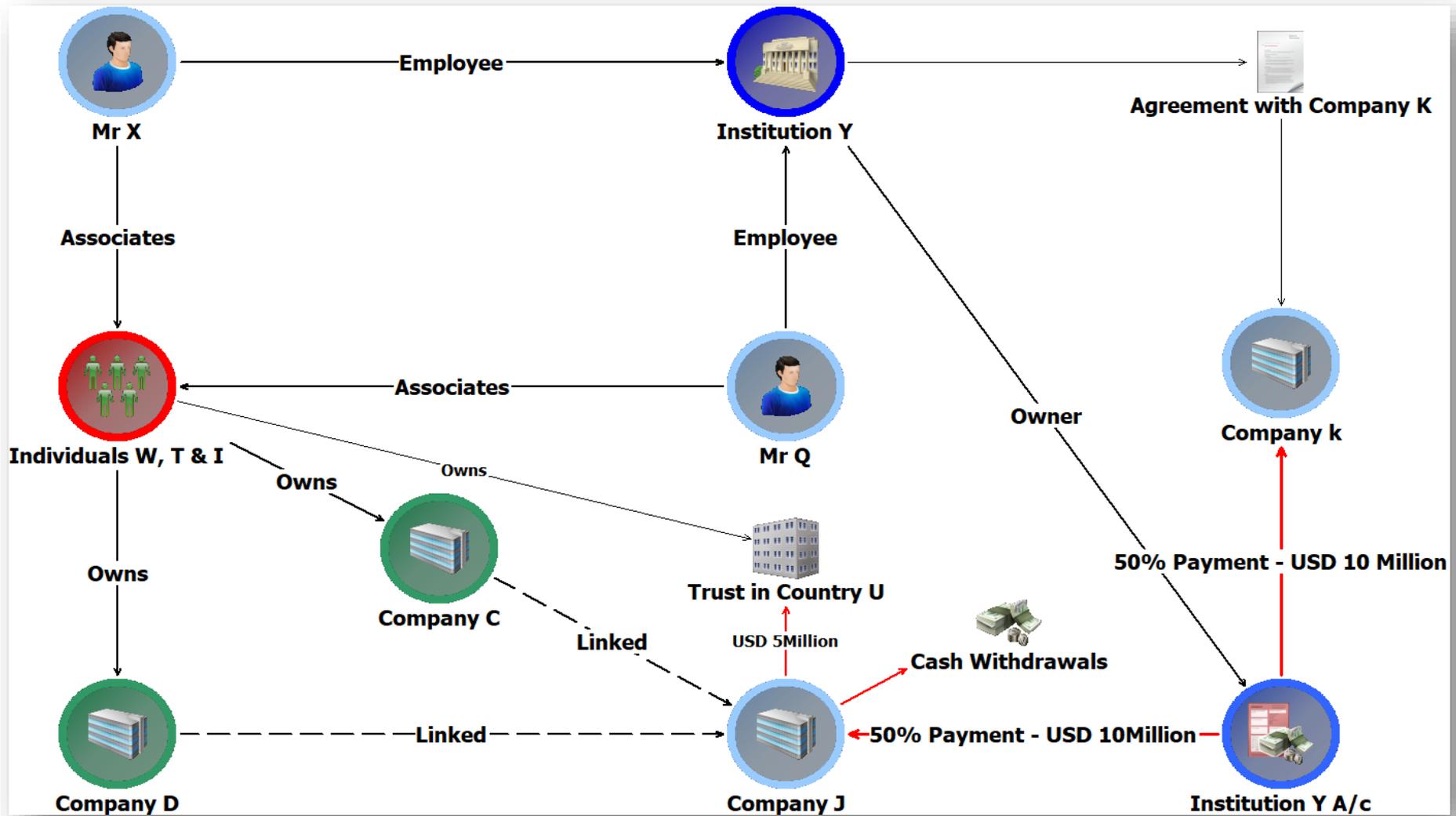
and **I**. The USD 5 million balance, which was supposed to be paid to **Company K**, was instead fraudulently paid to **Company J**. The duo working with accomplices **W**, **T** and **I** obtained an order to divert the USD 5 million balance from **Company K** to **Company J**. The final installment of USD 5 million paid to **Company J** was purportedly made on behalf of **Company C** and **Company D** owned by individuals **W**, **T**, and **I**.

Analysis revealed that the funds were fraudulently paid to parties that were not supposed to be the recipients. These funds were immediately transferred to other companies related to the suspects in Zambia and in an offshore jurisdiction.

The matter was therefore disseminated to the relevant LEA. The case was under investigations.

Chart 9 below illustrates suspected fraud and corruption.

Chart 9: Suspected fraud and corruption



Case Study XI: Suspected Fraud and Theft of Public Funds

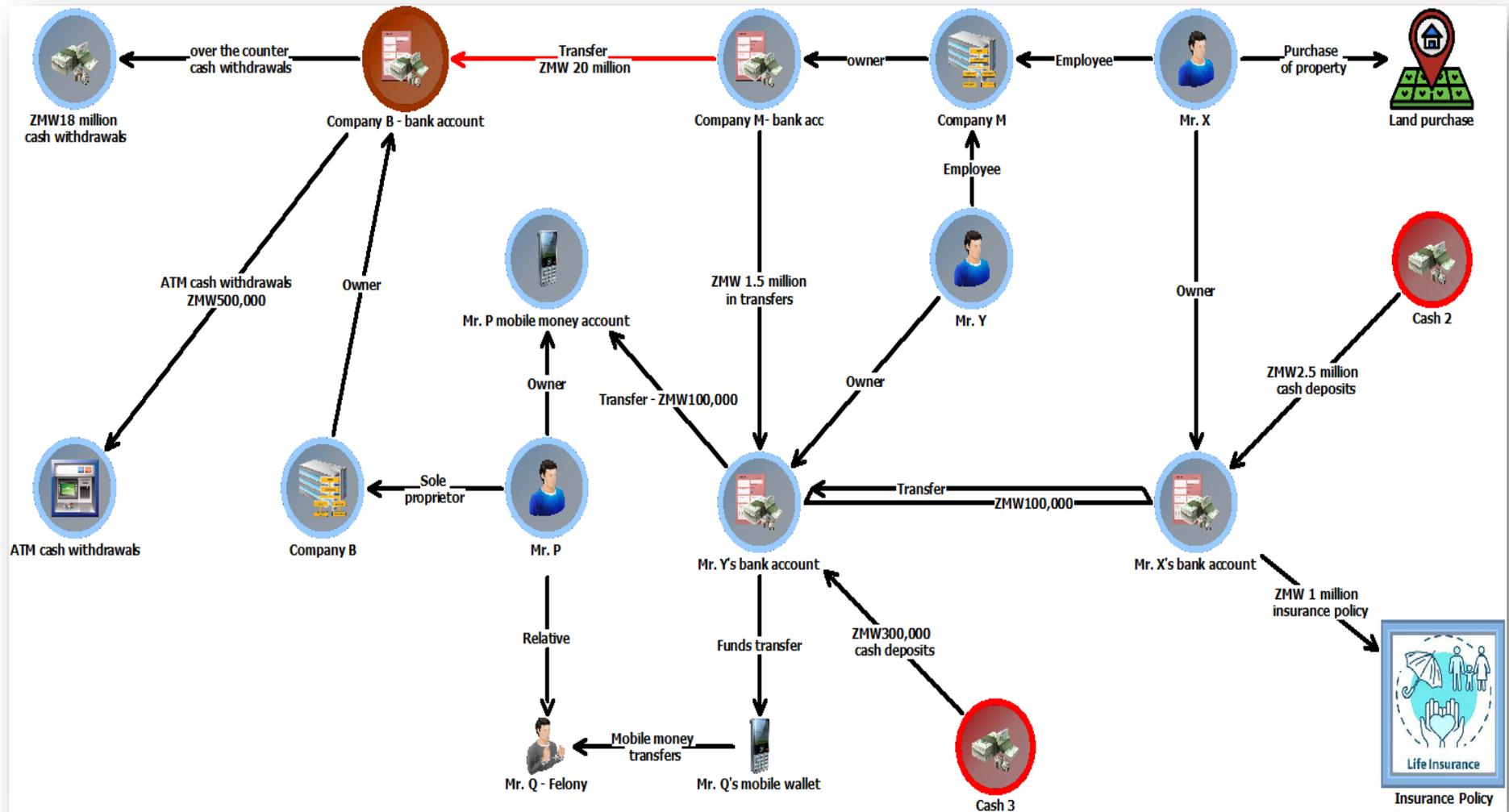
The FIC analysed a suspicious transaction report on suspected fraud and theft of public funds from **Company M**, a public institution.

Analysis established that individuals **X** and **Y** both individuals employed by **Company M**, had fraudulently transferred funds from the company's accounts to a shell company, **Company B**, solely owned by individual **P** an associate of individuals **X** and **Y**. Further analysis established that over a period of 1 year, individuals **X** and **Y** syphoned over **ZMW 20 million** from **Company M** to **Company B**. The funds were transferred with descriptions indicating payments for service delivery and statutory obligations to multiple companies. Over 90% of the funds were withdrawn as cash by individual **P**. It was noted that Individuals **X** and **Y**'s personal bank accounts had received multiple cash deposits during the same period of time. Further, individual **X** and **Y** were noted to have been transferring funds between their personal accounts. Individual **X** invested some of the funds in insurance policies and purchase of property. It was also established that individual **Y** remitted funds to individuals **P** and **Q** through mobile money wallet transfers.

In addition, the analysis revealed that another individual, Individual **Q**, a close associate of Individual **P**, had committed a felony. The matter was disseminated to the relevant LEA on suspected fraud, money laundering and corruption. The case was under prosecution.

Chart 10 below illustrates suspected fraud and theft of public funds.

Chart 10: Suspected fraud and theft of public funds



Case Study XII: Suspected Corruption

The FIC analysed a suspicious transaction report in 2021 relating to **Company D** which was awarded a contract in 2019 worth **ZMW 350 million** by a public institution for infrastructure development in the construction sector. The contract was to run for a period of 18 months. The suspicious transaction report was analysed and discontinued due to insufficient information. However, in 2024, the FIC received additional information on this case that required further analysis.

Analysis established that **Company D** was paid a down payment of **ZMW 75 million** by the public institution. Verifications on the project revealed that there was no evidence to show that works had been executed despite **Company D** receiving the down payment.

Further analysis revealed that **Company D** subcontracted 10 Zambian companies, to carry out ancillary works on the project. These companies were paid in excess of **ZMW 10 million** by the public institution despite works not being executed. Additional analysis revealed that **Company D** was awarded another contract worth **ZMW 45 million** by the same public institution in another part of the country but did not execute the works.

The case was disseminated to the relevant LEAs on suspected corruption and money laundering. The case was under investigations.

Recommendation on suspected corruption:

- i. Enhance verification controls for completion of works before payment.

Case Study XIII: Abuse of Corporate Vehicles for Suspected Public Sector Corruption

The FIC analysed a STR involving **Company ZO** (a foreign based company) that was awarded a contract by the Zambian Government in 2016. Analysis revealed that **Company ZO** had links with **Company G** (a local company). **Company G** was owned by **Director CZ** and **EZ**. **Company G** had four subsidiaries namely **Company KH**, **Company ET**, **Company SC** and **Company SM**. Government made multiple payments totaling USD43 million to **Company ZO** between 2016 and 2019.

Analysis of the transactions revealed that **Company ZO** had transferred in excess of **USD 100 million** to companies **KH**, **ET**, **SC** and **SM** from 2018 to 2019.

Over USD 40 million of these transfers were broken down as below:

- i. **Company KH** received USD 11 million;

- ii. **Company ET** received USD 14.2 million;
- iii. **Company SC** received USD 4 million; and
- iv. **Company SM** received USD 14.4 million.

The funds were utilized as follows:

- i. The **Directors CZ** and **EZ** of **Company G**, which was the holding company for companies **KH, ET, SC** and **SM** made various transfers and cash withdrawals in excess of USD24 million. Of the USD24 million, USD12.3 million was transferred directly to **Directors CZ** and **EZ** of **Company G**;
- ii. **Company ET** made a transfer of USD113,000 to a Prominent Influential Person (PIP) for acquisition of a farm;
- iii. **Company ET** made a transfer of USD850,000 to a bank account of an accommodation facility, whose beneficial owner was a PIP; and
- iv. A fund transfer of USD2 million was made by **Company G** to an associate company that invested the money in real estate. The beneficial owner of the real estate was a PIP.

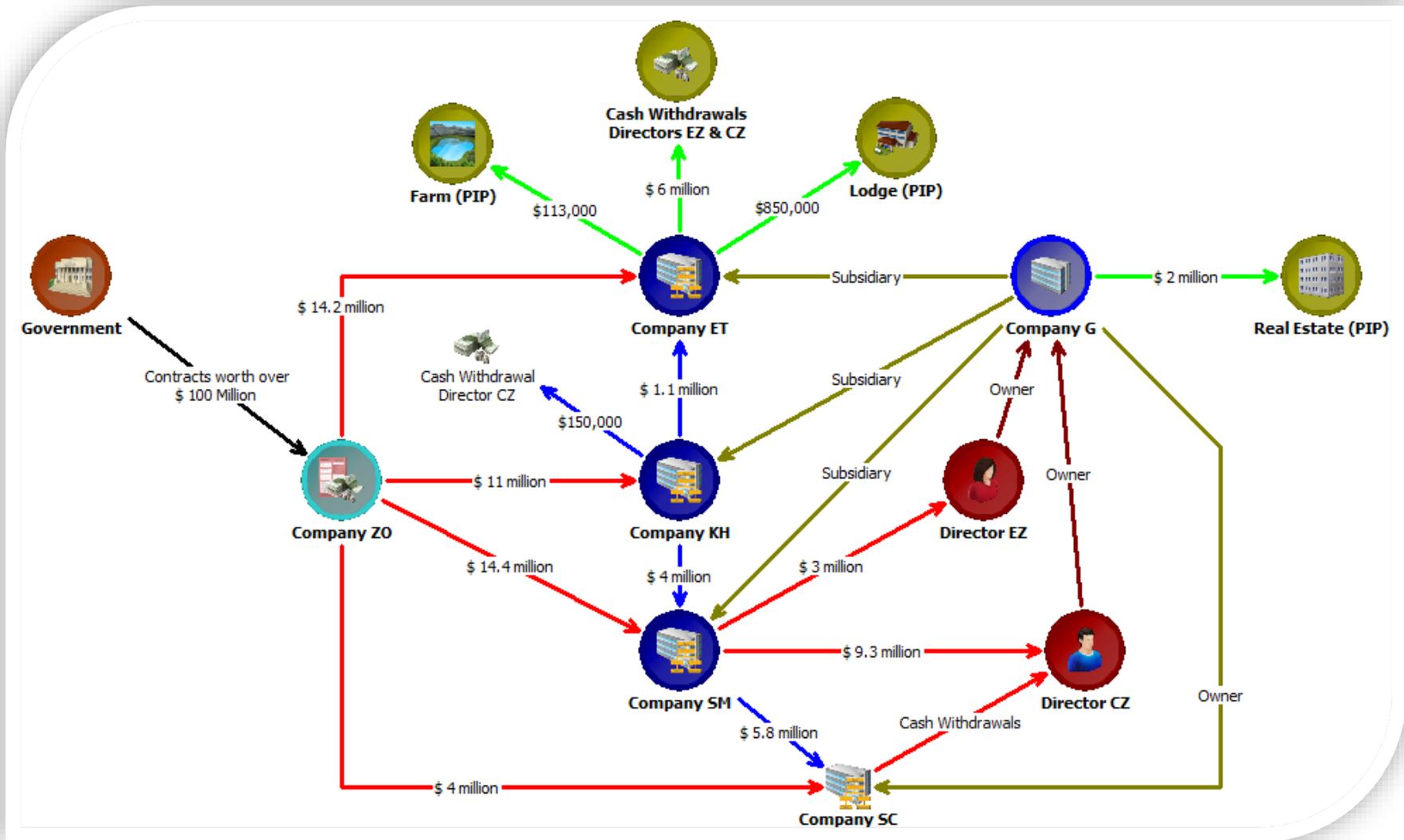
Further analysis revealed that **Company ZO** received a number of contracts from the Zambian Government. Our inquiries revealed that **Company G** and its subsidiaries were not compliant for tax purposes.

In 2020, these companies were de-risked by a financial institution where they maintained bank accounts. Based on the above findings, the matter was disseminated on possible tax evasion, corrupt practices and money laundering to various LEAs. The case proceeded to court.

The case was investigated by LEAs and assets worth USD 2.5 million were forfeited to the state in 2024.

Chart 11 below illustrates abuse of corporate vehicles for suspected public sector corruption.

Chart 11: Abuse of Corporate Vehicles for Suspected Public Sector Corruption



The case demonstrates a full cycle of intelligence gathering, investigation and prosecution leading to recovery of assets linked to proceeds of crime.

CHAPTER 3: SUPERVISION

3.1. SUPERVISION ACTIVITIES

The Centre is required to supervise reporting entities for compliance with their obligations under the FIC Act. Supervision of reporting entities is undertaken through inspections (on-site and off-site), training and awareness programmes, issuance of guidelines and directives.

3.1.1. On-site Inspections and Monitoring

During the year 2024, the Centre undertook on-site and off-site inspections in line with section 11A and 11B of the FIC Act. The on-site inspections were conducted on 55 reporting entities compared to 28 in 2023.

Table 1: On-site inspections conducted 2022-2024

Sector	No. of Entities 2024	No. of Entities 2023	No. of Entities 2022
Banking	4	1	3
Money or Value Transfer services	1	1	-
Real Estate Agents	3	7	-
Accounting and Audit Firm	14	-	-
Casino	4	15	-
Precious Stones and Metals	2	4	-
Legal Practitioners	26	-	-
Pensions and Insurance companies	1	-	-
Total	55	28	3

The table below depicts the monitoring activities conducted during the period under review.

Table 2: Monitoring activities conducted 2022-2024

Sector	Supervisory Tool	2024	2023	2022
Money or Value Transfer Service	Post monitoring reviews	13	9	13
Bureau De Change	Post monitoring reviews	47	63	63
Real Estate Agents	Off-site monitoring	-	-	15
	Post monitoring reviews	32	14	14
Accounting and Audit firms	Off-site monitoring	-	24	-
	Post monitoring reviews	115	63	63
Casino	Post monitoring reviews	30	20	20
Precious stones and metals	Post monitoring reviews	13	13	14
Legal Practitioners	Off-site monitoring	-	13	75
	Post monitoring reviews	119	75	-
Non-Bank Financial Institutions	Off-site monitoring	36	-	-
Pensions and Insurance companies	Off-site monitoring	9	-	-
Virtual Asset Service providers	Off-site monitoring	2	-	-
Total Number		416	294	277

Note: The post monitoring reviews undertaken in 2024 were follow-up activities on reporting entities monitored in previous years.

3.1.2. Compliance Barometer

The compliance barometer offers a concise overview of the state of AML/CFTP compliance programmes across sectors supervised by the FIC. It assesses the sectors' technical adherence to the requirements of the FIC Act but does not reflect the effectiveness of compliance implementation by reporting entities. The compliance barometer shows that the banking sector still has the highest levels of technical compliance with AML/CFTP requirements, with 93% of the sector assessed as having developed a compliance programmes. The FIC observed that there were improvements in technical compliance levels by accounting firms and Bureau de change in 2024 compared to 2023 as depicted in Charts 12 and 13 below.

Chart 12: Compliance Barometer 2024 and 2023

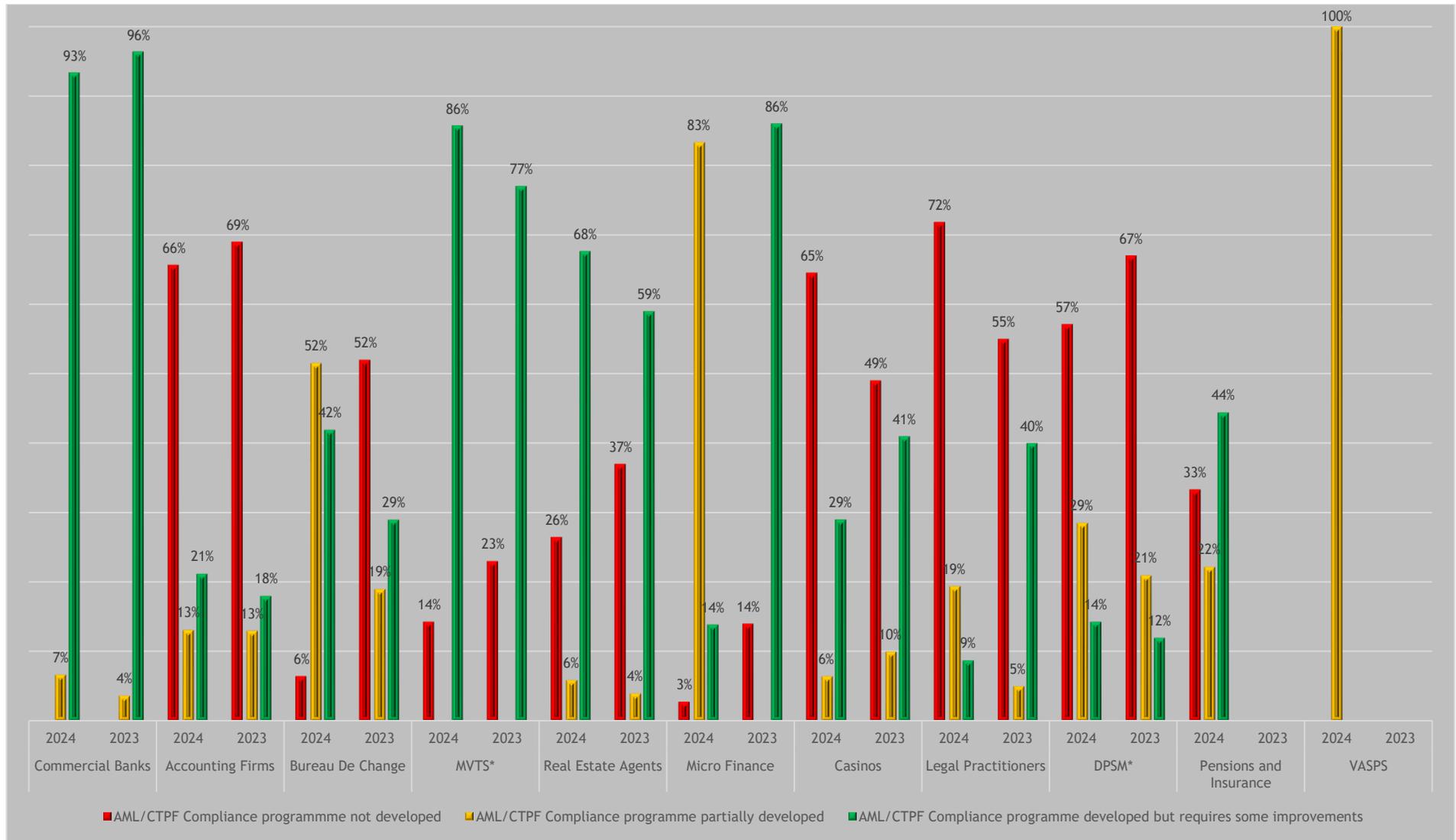
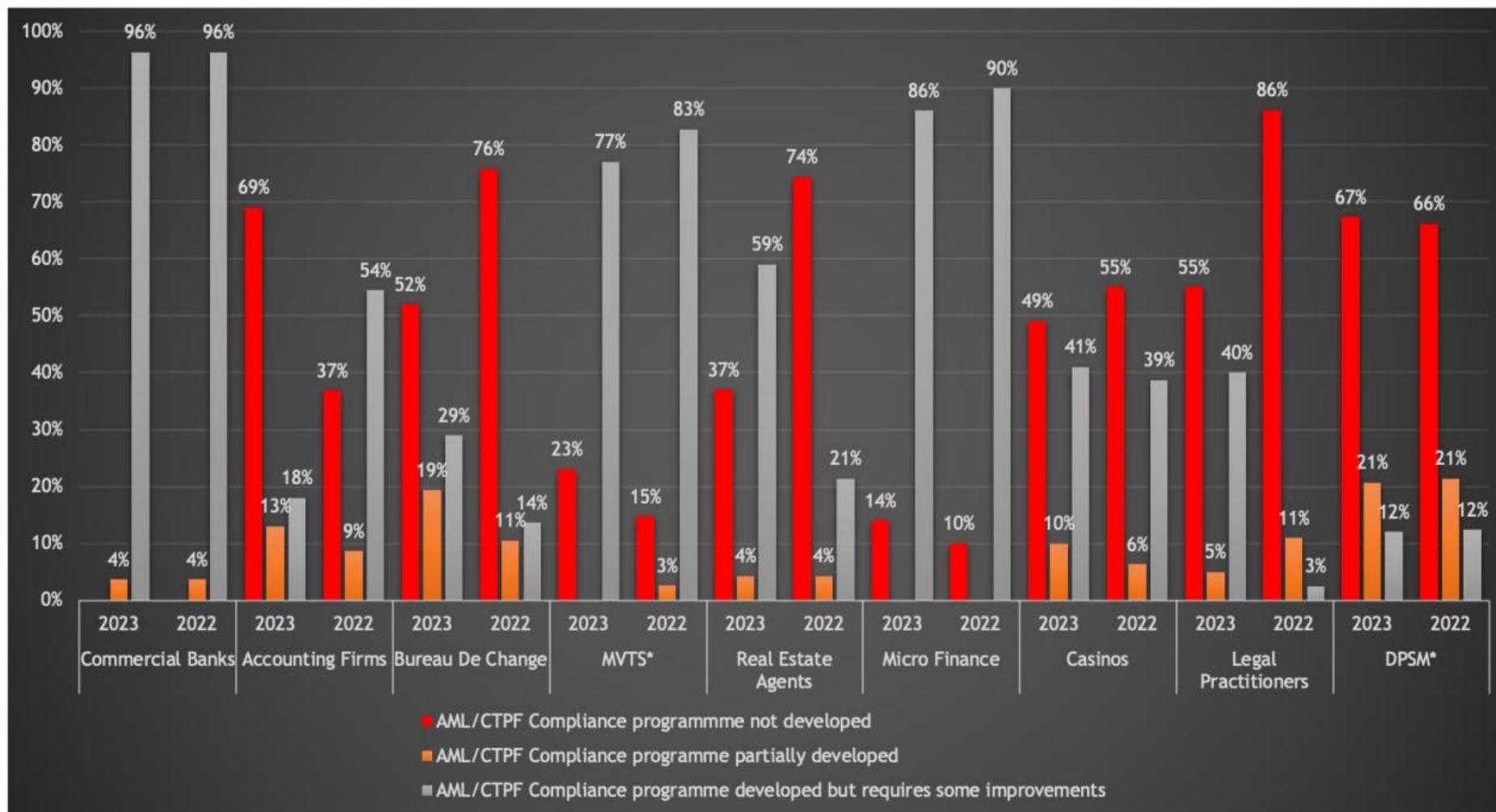


Chart 13: Compliance barometer 2023 and 2022



The Real estate sector, Money Value Transfer Service Providers (MVTs) and the dealers in precious stones and Metals (DPSM) also showed some level of improvements in their AML/CFTP compliance programme in 2024 compared to 2023. The Microfinance sector, Legal practitioners' sector and the Casinos sector showed lower levels of technical compliance in 2024 compared to 2023. The lower levels of technical compliance in 2024 were attributed to the increased number of monitored entities that were found to have deficiencies due to the non-implementation of certain requirements under the compliance programme. In 2024, the Barometer included two new sectors that were not covered in 2023 namely VASPs and the Insurance sector.

During the period under review, the Centre noted the following deficiencies:

- i. incomplete Customer Due Diligence;
- ii. non-reporting of STRs and CTRs;
- iii. none sanction screening of customers;
- iv. inadequate risk assessments; and
- v. lack of independent AML/CFTP audits.

3.1.3. Sanctions

During the period under review, the Centre imposed sanctions (monetary penalty) amounting to ZMW 1.2 million on non-compliant reporting entities in both the financial and DNFBP sectors. The ZMW1.2 million was paid and remitted to the Treasury. The major violations included failure to fulfil due diligence obligations, failure to comply with reporting obligations, inadequate ML/TF risk assessments, lack of sanction screening, lack of AML/CFTP independent audit and failure to maintain records. The sanctions are being reviewed to make them more dissuasive and proportionate.

3.2. AWARENESS AND TRAINING

3.2.1. Education and Awareness Activities

The Centre carried out awareness activities for various stakeholders in the private and public sectors to increase their knowledge on the Centre's mandate and to educate reporting entities and accountable institutions on their obligations under the FIC Act. During the period under review, the Centre conducted awareness sessions for a total of 2,543 participants representing 55 institutions from the following sectors: bureau de change, virtual asset service providers, motor vehicle dealers, travel agents, real estate, insurance, casinos, MVTs and financial institutions among many others as depicted in table 3.

Table 3: Awareness and Education Activities

Year	2024	2023	2022
Total	2,543	1,574	1,704

The Centre provided a series of specific training sessions for mobile money agents in conjunction with the Zambia Information and Communications Technology Authority (ZICTA) and LEAs in Lusaka province.

The Centre further collaborated with the financial sector regulators to conduct awareness sessions during their sector wide compliance forums. Further, the Centre had several media and public engagements which included featuring on radio and television programmes, and participation in annual general meetings of professional bodies. In addition, the Centre held sessions with senior government officials on IFFs in 4 Ministries.

3.2.2. Appointment of Compliance Officers

In the period under review, 112 Compliance Officers of reporting entities were approved by the Centre. In addition, the Centre approved the appointment of 28 Money Laundering Reporting Officers (MLROs), appointed by financial institutions to assist the Compliance Officers in fulfilling the reporting obligations of the institutions. The Centre noted an increase in the appointment of Compliance Officers in the DNFBS sectors as a result of increased awareness, supervision and enforcement activities in the same period. Table 4 below depicts the number of compliance officers approved over a period of three years.

Table 4: Compliance officers approved by the Centre

Year	2024	2023	2022
Compliance Officers	112	154	279

3.2.3. 2nd ML/TF/PF National Risk Assessment

Following Cabinet's approval to undertake the 2nd round of ML/TF/PF NRA in September, 2023, the Centre continued to coordinate the NRA exercise in 2024. The activities undertaken included the establishment of working groups, development of data collection tools, data collection and analysis. The results of the NRA will assist competent authorities and other stakeholders to be more focused in the application of resources to address ML/TF/PF risks.

CHAPTER 4: STATISTICS

The Centre receives reports from reporting entities and competent authorities pursuant to Sections 29, 30 and 38 of the FIC Act. Sections 29 and 30 of the FIC Act require reporting entities to submit STRs and Currency Transaction Reports (CTRs), respectively. In addition, according to Section 38 of the FIC Act as read with Regulation 8 of the FIC (Prescribed Threshold) Regulations, 2022, the FIC receives:

- i. Cross Border Currency Declaration Reports (CBCDRs) from the Zambia Revenue Authority. CBCDRs are reports declared to the Zambia Revenue Authority by individuals entering or leaving Zambia with an amount in cash, bearer negotiable instruments or both, exceeding the Kwacha equivalent of USD 5,000, whether denominated in Kwacha or any foreign currency;
- ii. Suspicious Transaction Reports are submitted on suspected or attempted money laundering, financing of terrorism or proliferation financing or any other serious offence;
- iii. Currency Transaction Reports are reports filed by reporting entities to the FIC in relation to any currency transaction in an amount equal to or above USD10,000 or kwacha equivalent;
- iv. Wire Transfer Reports are filed to the FIC by the Bank of Zambia in accordance with Section 26 of the FIC Act; and
- v. Spontaneous Disclosure Reports (SDR) are received from competent authorities such as law enforcement agencies, supervisory authorities and foreign financial intelligence units. In addition, individuals and corporates submit reports to the FIC on a voluntary basis.

Table 5: Number of reports received over a period of 3 years

Year	Number of reports received		
	2024	2023	2022
STRs	8,981	10,293	5,745
SDR	83	78	62
CTRs	377,808	285,004	239,717
CBCDRs	2,888	3,421	4,025

4.1. SUSPICIOUS TRANSACTION REPORTS

4.1.1. Suspicious Transactions Reports Received

In 2024, the Centre received a total of **8,981** STRs, representing a decrease of 12.74% compared to the **10,293** in 2023. The common reasons for suspicion identified in the STRs received in 2024 were unusually high USD-denominated cash deposits, structured deposits below the reporting thresholds, transactions inconsistent with customer profile, immediate international remittance following cumulation of funds, and use of Zambian owned companies and personal accounts to conceal beneficial ownership. These trends and the reasons for suspicion observed in 2024 were consistent with those observed in 2023 and 2022.

Chart 14: STRs received over a 3-year period



The continued reliance on cash in the economy presents significant money laundering (ML) risks due to its anonymous nature, which makes it difficult to trace and monitor transactions. Cash transactions are often used to obscure the source and destination of illicit funds, posing challenges for financial institutions in detecting suspicious activity. The high usage of cash in transactions amplifies the potential for misuse, as it enables individuals to circumvent regulatory controls and engage in financial crimes without drawing immediate scrutiny. The common reasons for filing STRs were large cash deposits and withdrawals, inconsistent with customer profile and unusual outward remittance. The table below shows reasons for filing STRs.

Table 6: Reasons for filing STRs

Reason for suspicion	Number of Reports		
	2024	2023	2022
Activity inconsistent with customer profile	654	737	433
Avoiding reporting obligations	668	688	187
Corruption	40	55	64
Fraud	484	401	239
Irregular or Unusual international banking activity	539	412	111
Large or unusual cash deposit	1,217	1,688	855
Large or unusual cash withdrawals	1,075	1,379	657
Large or unusual inward remittance	736	1,043	821
Large or unusual outward remittance	1,105	1,304	725
Many third parties making deposits into the account	383	521	173
Other	38	102	20
Person - Suspicious Behavior	537	627	423
Phishing (Electronic Fraud)	111	257	118
Sudden unexpected activity on previous dormant	117	184	121
Unusual business practices	557	407	555
Unusually large foreign currency transaction	687	477	234
Watch listed individual/organization	33	11	9
Total	8,981	10,293	5,745

4.1.2. Suspicious Transaction Reports received by type of reporting entity

Commercial banks continued to be the highest reporting institutions of STRs with **8,710** reports received in 2024 representing 96.9% of the total STRs. In a comparative analysis, it was observed that the number of STRs had decreased by 13.5% from **10,072** STRs reported in 2023. The MVTs providers accounted for the second highest source of STRs after commercial banks at **184** compared to **163** in 2023. In 2024 there were three registered VASPs in Zambia. The VASPs reported 35 STRs to the Centre in 2024, which is an increase from 11 STRs in 2023.

In 2024, the Centre observed that casinos had filed 17 STRs to the Centre. This is in contrast to none reported in 2023. The none reporting of STRs in 2023 and the subsequent increase in 2024 can be linked to heightened awareness and enhanced supervision efforts by the Centre. Other DNFBPs such as law firms, accounting firms, real estate agents and dealers in precious stones and minerals, and trust and company service providers did not submit STRs to the Centre in 2024.

Table 7: Number of STRs received by type of reporting entities

Sector	Number of reports received by type of reporting entities over a 3-year period		
	2024	2023	2022
Commercial banks	8,710	10,072	5,574
MVTS Providers	184	163	144
Microfinance	20	43	8
Casinos	17	0	15
Accounting firms	0	0	2
Law firms	0	0	0
Insurance	3	4	0
Bureau de Change	1	0	0
Virtual Asset Service Provider	35	11	0
Building Societies	9	0	0
Motor vehicle dealers*	1	0	2
Unit Trusts	1	0	0
Total	8,981	10,293	5,745

*Motor vehicle dealers are designated as accountable institutions in the FIC Act.

4.1.3. Suspicious Transaction Reports Analysed

During the period under review, the Centre analysed a total of **18,330** reports, some of which were received in prior years. This reflected a 16.8% increase from the **15,696** analysed in 2023. Out of the 18,330 reports analysed, **17,379** reports were closed on account of low risk and verification establishing that transactions were legitimate.

4.1.4. Financial Intelligence Reports Disseminated

The number of disseminated financial intelligence reports to the LEAs and foreign competent authorities increased from **923** in 2023 to **951** in 2024, representing a 3% increase.

Chart 15: Number of disseminated cases 2022-2024

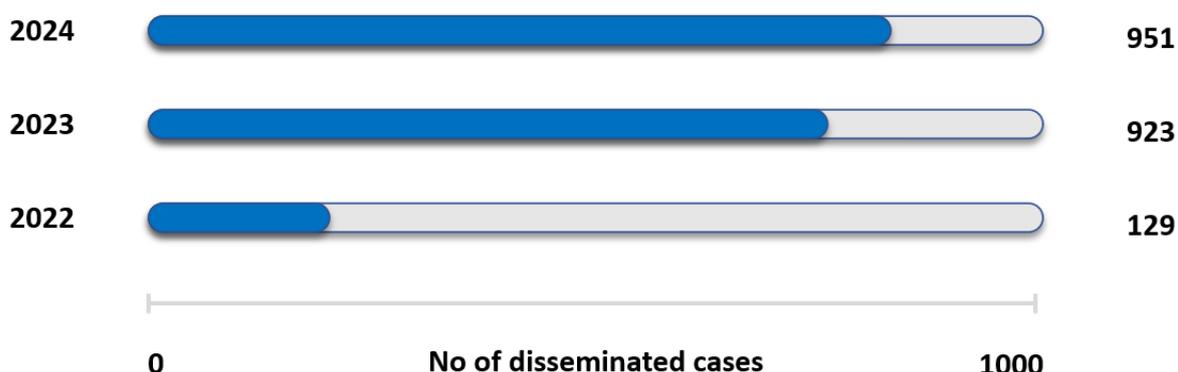


Table 8 below provides a comparison of disseminations over a 3-year period:

Table 8: Intelligence Reports disseminated

Suspected Offence	Number of Reports Disseminated		
	2024	2023	2022
Corruption	10	9	10
Fraud	63	6	4
Money laundering	243	11	44
Tax evasion	573	450	52
Terrorism financing	5	0	11
Violations of the Banking and Financial Services Act	2	443	8
Violation of Immigration and Deportation Act	55	4	0
Grand total	951	923	129

In terms of the involved potential predicate offence or typology in intelligence disseminated over the past three years, tax crimes remained at the top of the list, followed by money laundering.

4.1.5. Feedback on Disseminated Intelligence Reports

During the period under review, the Centre disseminated **951** intelligence reports to various LEAs. Out of which 573 were disseminated to the Zambia Revenue Authority (ZRA) who made tax assessments worth **ZMW 28.9 billion** from 326 reports.

Feedback received from other LEAs on disseminated reports indicated that 3 convictions and 7 non-conviction-based forfeitures were secured, resulting in the forfeiture of assets valued at **USD 26.5 million** and **ZMW 71.5 million** in properties and cash.

4.1.6. Freezing of Bank Accounts

Section 10(3) of the FIC Act grants the Director General the authority to order a reporting entity to freeze an account or suspend a transaction if there is reasonable suspicion of money laundering, financing of terrorism, proliferation, or other serious offenses. The freezing of an account or suspension of a transaction can last for a maximum of fifteen days.

During the period under review, the Centre froze 34 bank accounts and 10 mobile money accounts with cumulative account balances of **USD 4.7 million** and **ZMW 176.9 million** compared to 27 bank accounts with cumulative bank account balances of **USD 2.8 million** and **ZMW 126.5 million** in 2023. The action was taken to facilitate inquiries by Competent Authorities.

4.2. CURRENCY TRANSACTION REPORTS

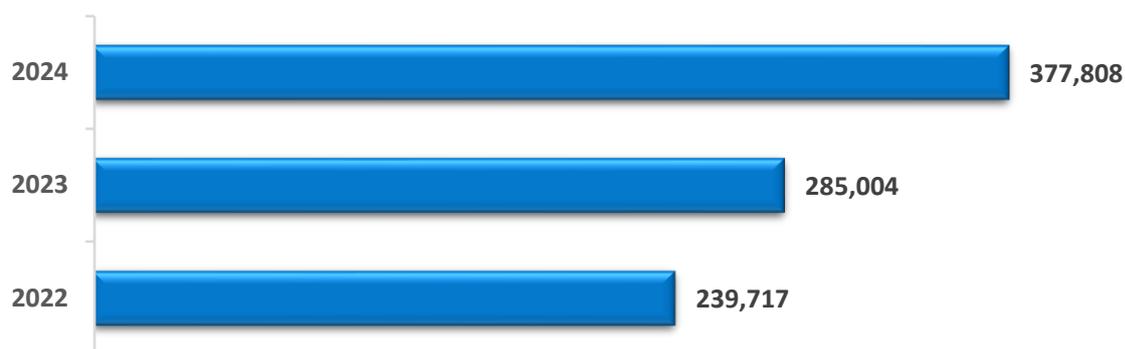
4.2.1 Currency Transaction Reports Received

In 2024, the Centre observed a 32.6% increase in the number of CTRs received, with the total rising to **377,808** from **285,004** in 2023. This growth was mirrored by a substantial rise in the value of CTRs, which surged to **ZMW 1,036.4 billion** in 2024 from **ZMW 501.66 billion** in 2023. This upward trend in both the volume and value of CTRs has been consistent in recent years.

The analysis of STRs revealed a significant proportion of cases involving large cash transactions that deviated from the customer's typical financial behavior. Further, it was noted that Lusaka, Zambia's commercial capital, accounted for the highest volume and value of these transactions, followed by the Copperbelt province, a region driven by extensive mining operations as shown in tables 8 and 9 respectively. These areas, with their robust economic activity, serve as key focal points for both legitimate and potentially illicit financial transactions.

Analysis of CTRs revealed that most were linked to suspected IFFs and foreign exchange trading, particularly in border regions, highlighting the increased vulnerability to cross-border financial crime in these high-activity zones. The porous nature of border areas makes them vulnerable for such financial behaviours, amplifying the risks associated with IFFs.

Chart 16: Number of CTRs received from 2022 to 2024



The table below depicts the number of corporate CTRs that were recorded during the period under review by province.

Table 9: Corporate CTRs by province

Province	Number of Transactions		
	2024	2023	2022
Central	6,509	4,952	4,188
Copperbelt	53,717	35,142	27,220
Eastern	5,820	5,493	4,053
Luapula	1,843	926	876
Lusaka	173,052	128,263	103,876
Muchinga	1,536	1,353	1,324
North Western	2,382	1,631	1,243
Northern	1,052	817	628
Southern	7,397	5,221	3,734
Western	676	778	703
Unclassified	5,778	1,029	1,098
Total	259,762	185,605	148,943

Table 10: Individual CTRs by province

Province	Number of Transactions		
	2024	2023	2022
Central	3,395	3,958	3,115
Copperbelt	24,751	21,671	18,042
Eastern	6,138	6,794	6,709
Luapula	442	471	489
Lusaka	66,004	51,524	40,913
Muchinga	6,061	3,163	3,428
North Western	1,891	1,374	670
Northern	2,155	1,170	902
Southern	4,108	5,176	2,910
Western	1,109	959	719
Unclassified	1,992	3,139	12,877
Total	118,046	99,399	90,774

4.3. CROSS BORDER CURRENCY DECLARATION REPORTS

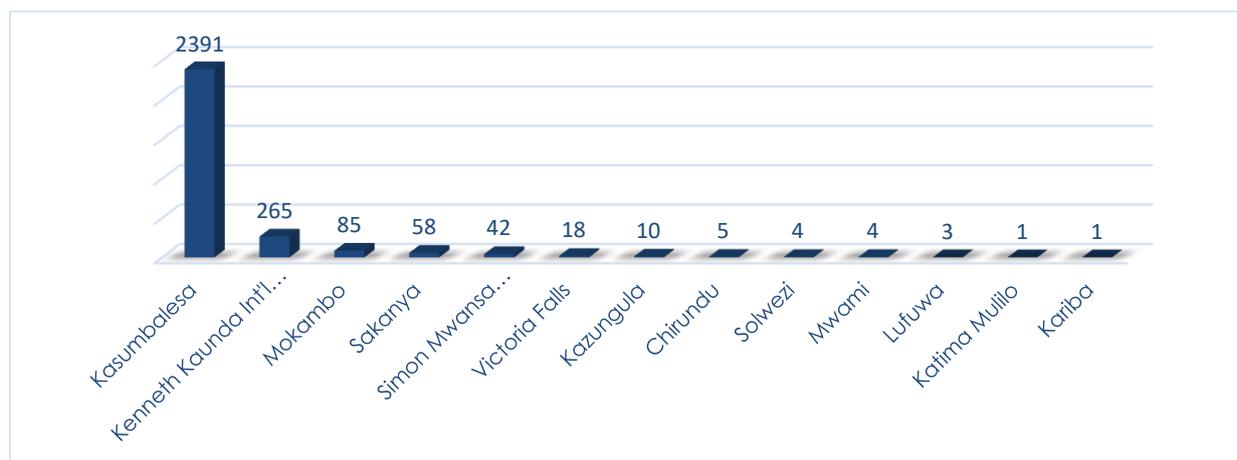
In 2024, the Centre received a total of **2,888** CBCDRs valued at **USD 411.9 million**, compared to **3,421** reports worth **USD 642.8 million** in the previous year. Section 41 (A) of the Customs Act as read with Section 38 of the FIC Act requires travelers to declare currency equal to or above USD 5,000 at points of entry or exit. This information is used by the Centre in the process of analysis.

Table 11: Cross Border Currency Declaration Reports by value and number

Year	Number of reports	Amount in USD (Millions)
2024	2,888	411.9
2023	3,421	642.8
2022	4,025	1,088.0

During the period under review, the Centre received CBCDRs from the following borders: Kasumbalesa, Sakanya, Kenneth Kaunda International Airport, Mokambo, Simon Mwansa Kapwepwe International Airport, Chirundu, Solwezi, Victoria Falls, Kazungula, Mwami, Kariba, Katima Mulilo and Lufuwa. The bulk of the reports received originated from Kasumbalesa border post with a total of 2,391 reports as shown in Chart 17 below.

Chart 17: Number of Declarations from 2022 to 2024



Kasumbalesa also accounted for a significant portion in value of all declarations received with 84% of the **USD 411.9 million** recorded. There were no CBCDRs received from Harry Mwanga Nkumbula and Mfuwe International Airports.

There were more declarations made by inbound travelers compared to outbound travelers in 2024. Of the declarations made, 67% were made by

inbound travelers while 9.8% of declarations were made by outbound travelers. A significant 23.2% of declarations were marked with a "null" status for arrival or departure.

Table 12: Inbound and Outbound Traveler Declarations

Year	Number of Declarations	
	2024	2023
Declarations made by inbound travelers	1,937	2,416
Declarations made by outbound travelers	282	298
Declarations where arrival/departure not stated	669	707

Table 13: Value of Cross Border Currency Declaration Reports Received

Year	Value of Declarations (USD)	
	2024	2023
Declarations made by inbound travelers	257,594,620.0	308,284,664.0
Declarations made by outbound travelers	11,552,578.0	22,555,172.0
Declarations where arrival/departure not stated	142,712,996.0	311,990,164.0

The declarations made in 2024 were made by travelers from 40 nationalities. The top 10 nationalities with the highest aggregate value of declarations in the period are as shown in Table 14 below.

Table 14: Top 10 nationalities with the highest value of declarations 2024

Nationality	Frequency	Aggregate Value (USD' million)
Democratic Republic of Congo	2,536	398.40
Zambia	212	8.35
India	21	1.15
Tanzania	8	0.61
Zimbabwe	15	0.47
Kenya	10	0.46
Guinea	2	0.42
Sierra Leone	1	0.34
South Africa	9	0.21
Botswana	5	0.18
Total		410.5

Table 15: Top 10 nationalities with the highest value of declarations 2023

Nationality	Frequency	Aggregate Value (USD' million)
Democratic Republic of Congo	2,930	627.25
Zambia	245	10.24
India	21	2.0
Kenya	8	0.53
Zimbabwe	15	0.50
Botswana	9	0.48
Tanzania	7	0.23
Malawi	7	0.22
Ghana	3	0.21
Total		642.00