



FINANCIAL INTELLIGENCE CENTRE

THE 9TH MONEY LAUNDERING AND TERRORISM FINANCING TRENDS REPORT 2023

*Tax Evasion, Corruption, Money Laundering and
Associated Illicit Financial Flows*

MONEY LAUNDERING AND TERRORISM FINANCING TRENDS REPORT
*Tax Evasion, Corruption, Money Laundering
and
Associated Illicit Financial Flows*

TABLE OF CONTENTS

List of Tables	iii
List of Charts	iv
Acronyms	v
Message from the Director General	vi
1.0 Background	1
1.1 Objectives of the Trends Report	2
i. Awareness	2
ii. Policy Formulation	2
iii. Supervision	2
1.2 Functions of the Financial Intelligence Centre	2
i. Strategic Analysis	2
ii. Tactical Analysis	2
iii. Dissemination	2
iv. Spontaneous Disclosure	2
2.0 Trends and Case Studies	3
2.1 Public Sector Corruption and Money Laundering	4
2.2 Use of Cash in Illicit Transactions	7
2.3 Masking Beneficial Ownership of Corporate Vehicles	9
2.4 Cyber enabled Financial Crimes	12
2.5 Abuse of Casinos for Money Laundering	13
3.0 Compliance Barometer and Awareness	15
3.1 Compliance Barometer	16
3.2 Awareness and Training	17
3.2.1 Education and Awareness Activities	17
3.2.2 Designation of Compliance Officers	17
3.2.3 National AML/CFTP Policy	17
3.2.4 2nd Money Laundering/Terrorist Financing/Proliferation Financing National Risk Assessment	18
4.0 Statistics	19
4.1 Sources of Information	20
4.1.1 Suspicious Transactions Reports Received	20
4.1.2 Suspicious Transaction Report received by Sector	21
4.1.3 Suspicious Transaction Reports Analysed	22
4.1.4 Intelligence Reports Disseminated	23
4.1.5 Feedback on Disseminated Intelligence Reports	24
4.1.6 Freezing of Bank Account	24
4.2 Currency Transaction Reports	25
4.2.1 Currency Transaction Reports Received	25
4.3 Cross Border Currency Declaration Reports	26
Working Definitions	29

LIST OF TABLES

Table 4.1: Number of reports received over a 3-year period	20
Table 4.2: STRs received by number and value over a 3-year period	21
Table 4.3: Number of STRs received by sector	22
Table 4.4: Intelligence Reports disseminated	23
Table 4.5: Status of cases disseminated	24
Table 4.6: Number of CTRs received from 2021 to 2023	25
Table 4.7: Corporate CTRs by province	26
Table 4.8: Individual CTRs by province	26
Table 4.9: Top 10 nationalities with the highest value of declarations	27
Table 4.10: Aggregate value of declaration based on ports of entry	27

LIST OF CHARTS

Chart 1: Anti Money Laundering and Countering Terrorism or Proliferation Financing Value Chain	2
Chart 2: Use of shell companies in public procurement corruption	5
Chart 3: Abuse of corporate vehicles for suspected public sector corruption	6
Chart 4: Abuse of corporate vehicles for suspected corruption	7
Chart 5: Use of corporate vehicles for suspected money laundering and illicit financial Flows	8
Chart 6: Use of cash in transactions to conceal fraudulent activities	9
Chart 7: Use of shell companies for corruption and money laundering	10
Chart 8: Abuse of corporate vehicles in ponzi scheme	11
Chart 9: Cyber enabled fraud involving a foreign jurisdiction	12
Chart 10: Cyber enabled fraud on multiple financial institutions	13
Chart 11: Compliance barometer	16

LIST OF ACRONYMS

AML/CTPF	Anti-Money Laundering/Countering Terrorism & Proliferation Financing
AML	Anti-Money Laundering
BO	Beneficial Ownership
CBCDRs	Cross Border Currency Declaration Reports
CTR	Currency Transaction Report
DNFBPs	Designated Non-Financial Businesses and Professions
ESAAMLG	Eastern and Southern Africa Anti Money Laundering Group
FATF	Financial Action Task Force
FIC	Financial Intelligence Centre
LEAs	Law Enforcement Agencies
ML	Money Laundering
ML/TF/PF	Money Laundering / Terrorism Financing / Proliferation Financing
MVTS	Money or Value Transfer Services
PIPs	Prominent Influential Persons
PF	Proliferation Financing
SDR	Spontaneous Disclosure Report
STR	Suspicious Transaction Report
TF	Terrorism Financing
VASPs	Virtual Asset Service Providers



MESSAGE FROM THE DIRECTOR GENERAL

The Financial Intelligence Centre (the FIC) marked its 10th year of existence in September 2023, having been operationalised in 2013. In 2014, the FIC produced its inaugural Money Laundering/Terrorism Financing Trends Report. The Trends Report was introduced to broadly support the strategic analysis function of the FIC.

Further, it was envisaged that the Trends Report would create awareness across the multiple stakeholders as regards typologies on financial crimes in the country. The Trends Report has evolved over the years and plays a critical role in serving as a source of information for policy makers, reporting entities and the general public. In its 9th year of publication, the Trends Report continues to evolve in content and approach to align with the dynamic financial crime landscape in Zambia.

In 2023, the FIC analysed 15,696 Suspicious Transaction Reports (STRs) (2022: 10,293) out of which 923 (2022: 129) intelligence reports were disseminated to Law Enforcement Agencies (LEAs). The value of disseminated intelligence reports was ZMW13.58 billion compared to ZMW5.83 billion in 2022 representing a 133 percent increase. The majority of intelligence reports disseminated were on suspected money laundering, corruption and tax evasion. This trend is consistent with previous years.

As a result of disseminations by the FIC, the Zambia Revenue Authority (ZRA) made tax assessments amounting to ZMW1.2 billion in principal tax, interest and penalties. As at the close of the year, ZRA had made recoveries of over ZMW3.5 million. Feedback received from other LEAs on disseminated reports indicated that the cases were at investigation and prosecution stages. Further, accused persons were convicted in some cases, while non-conviction based forfeitures were recorded in others.

The abuse of corporate vehicles was a continuing trend in 2023. This was done by masking of beneficial ownership through various schemes such as usage of fronts and falsified documents. In majority of the cases, corporate vehicles had either not disclosed their beneficial owners with the Patents and Companies Registration Agency (PACRA) as required by the Companies Act No. 10 of 2017 or disclosed 'strawmen' as beneficial owners.

The FIC continued to observe the trend in the use of cash to conceal the source of illicit funds and creation

of some level of anonymity in the transactions. Despite the increase in the availability of electronic payment channels, the FIC through its analysis observed an upward trend in the use of cash.

In 2023, the FIC analysed 15,696 STRs out of which 923 intelligence reports were disseminated to Law Enforcement Agencies

The casino sector had also experienced heightened levels of vulnerability to money laundering and other financial crimes. Through its analysis and supervision activities, the FIC observed that casinos would deliberately adopt an operating business model that was heavily reliant on cash transactions and as a consequence leave no audit trail. In this cash environment, some casinos facilitated the payment of bribes and possible understatement of their income. Further, intelligence gathered indicated that some casinos engaged in illegal cross border cash courier business.

In the period under review, the FIC developed the 2024-2026 Strategic Plan themed "Consolidating the gains through leveraging emerging technologies". Over the 10 years of existence, the FIC made significant gains in executing its mandate and contributing towards ensuring that Zambia has a stable financial system that is resilient to financial crimes. Despite the gains made, there is still work to be done in the fight against financial crimes in Zambia to ensure that the progress is not eroded. In this context, the FIC will within this strategic planning period leverage emerging technologies to consolidate and build on the gains attained so far.

With the continued support from the Government and collaboration with stakeholders, the FIC remains resolute in discharging its mandate.



Clement K. Kapalu
DIRECTOR GENERAL
FINANCIAL INTELLIGENCE CENTRE



CHAPTER 1: **BACKGROUND**

1.1 OBJECTIVES OF THE TRENDS REPORT

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

- i. **Awareness:** provide awareness by educating the public and reporting entities of their obligations and informing them of measures to detect, prevent and deter Money Laundering/Terrorism Financing/Proliferation Financing (ML/TF/PF) or any other serious offences relating to ML/TF/PF.
- ii. **Policy Formulation:** based on observed trends, inform government policy formulation.
- iii. **Supervision:** facilitate effective risk-based supervision and enforcement of anti-money laundering, countering of terrorism or proliferation financing (AML/CTPF).

The functions of the FIC as provided under section 5 of the Financial Intelligence Centre Act No. 46 of 2010 (as amended) are inter alia to:

- i. **Strategic Analysis:** conduct strategic analysis to identify trends and patterns relating to ML/TF/PF or any other serious offence relate to ML/TF/PF.

- ii. **Tactical Analysis:** receive, request, analyse and evaluate suspicious transaction reports and information from any other source authorised under any written law to make a suspicious transaction report including a designated foreign authority to determine whether there are reasonable grounds to transmit reports for investigation by law enforcement agencies or designated foreign authorities.
- iii. **Dissemination:** disseminate information, spontaneously or on request, to law enforcement agencies and other competent authorities, where there are reasonable grounds to suspect money laundering or financing of terrorism or proliferation and other financial crimes.
- iv. **Spontaneous Disclosure:** provide information relating to suspicious transactions to any designated foreign authority, subject to conditions that the Director General may determine, in accordance with the FIC Act.

Chart 1: Anti Money Laundering and Countering Terrorism or Proliferation Financing Value Chain





CHAPTER 2:
TRENDS AND CASE STUDIES

2.0 TRENDS AND CASE STUDIES

In 2023, the FIC observed continuing and emerging trends in financial crimes in the country. This section of the report highlights both continuing and emerging trends with accompanying case studies.

Continuing trends were mostly observed in the following areas: public sector corruption and money laundering, use of cash in illicit transactions and masking beneficial ownership of corporate vehicles, while emerging trends were observed in cyber enabled financial crimes and abuse of casinos for money laundering.

2.1 PUBLIC SECTOR CORRUPTION AND MONEY LAUNDERING

During the period under review the FIC analysed STRs that involved suspected public sector corruption. The reports bordered on suspected abuse of office and procurement corruption.

Further, the FIC observed a continuing trend of companies and individuals linked to prominent influential persons being awarded fraudulent procurement contracts.

The red flags associated with public sector corruption include:

- i. Overpricing of contract sum;
- ii. Non-delivery of contract obligation;
- iii. Failure to follow procurement procedures;
- iv. Failure to disclose conflict of interest;
- v. Facilitation payments;
- vi. Selective quick processing of tenders and payments; and,
- vii. Award of contract to newly incorporated entities.

Case Study I: Use of Shell Companies in Public Procurement Corruption

The Centre analysed a STR on suspected corrupt practices against Company AD (foreign based) and Company R (a group of companies). The matter related to the award of a contract of USD 100 million to construct infrastructure by Ministry S.

In 2012, Ministry S signed a contract with Company AD for the design, rehabilitation and building of government infrastructure units across the country. It was noted that at the time the contracts were awarded to Company AD, it had only been in existence for one year.

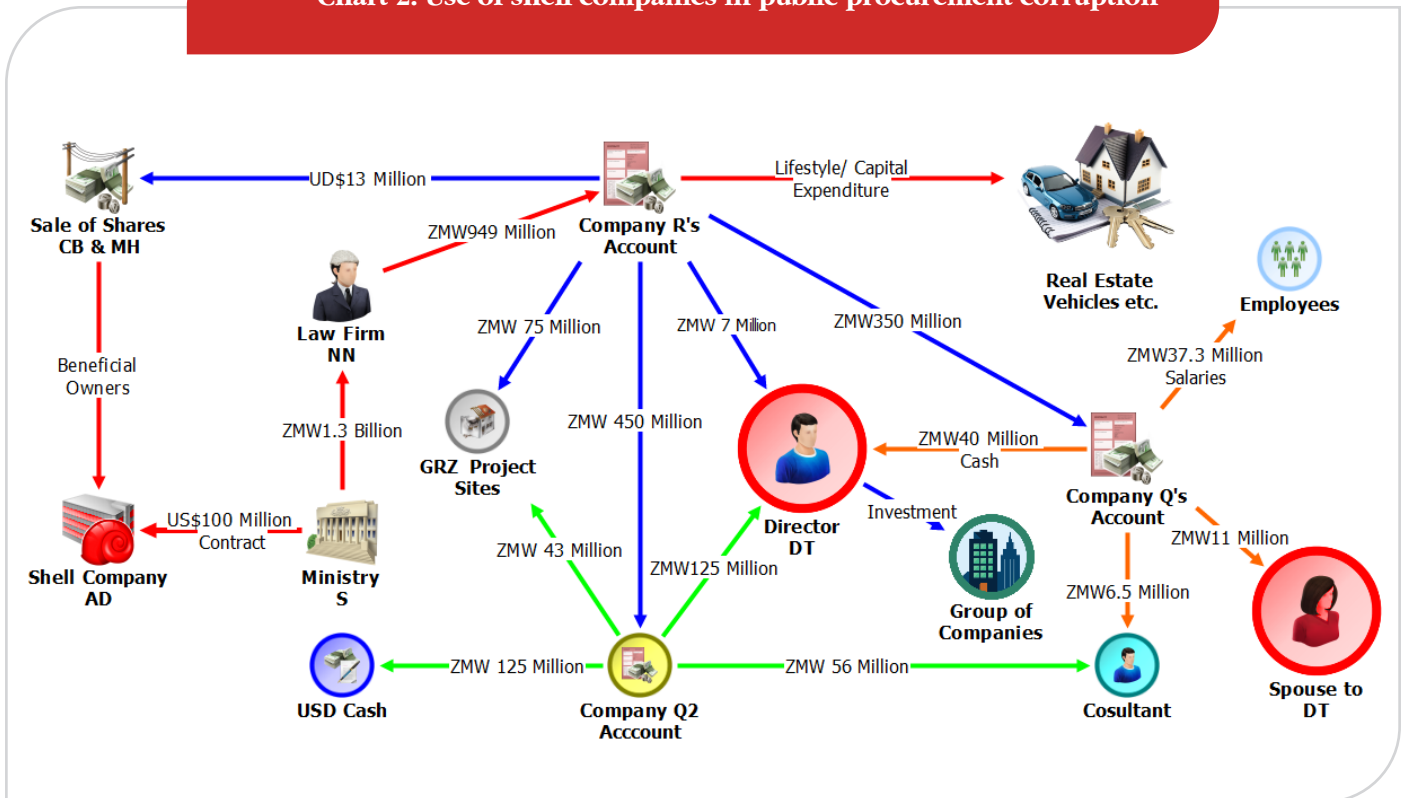
The observations in summary;

- i. The inquiry noted that in 2017, Company AD introduced Company R as its partner in the construction of the government infrastructure.
- ii. In 2017, Ministry S changed the financing model of the contract from Public Private Partnership (PPP) to direct Government funding and in 2018, Ministry S made a payment of ZMW 1.3 billion to Company R. This payment was made through law firm NN. Law firm NN made a transfer of ZMW949 million to Company R.
- iii. Company R made the following transfers: Company Q a subsidiary of Company R received ZMW350 million; Company Q2 a subsidiary of Company R received ZMW450 million; ZMW 75 million towards the government infrastructure project; USD13 million to individuals in an offshore center in Africa; and, ZMW7 million to Director DT, who was a shareholder of Company R.
- iv. It was established that as at December 2023, the contract works had not been fully executed.
- v. Analysis revealed that Company AD was a shell company. Further, analysis revealed that some of the funds paid through law firm NN were utilised to purchase a farm, construct residential houses, purchase vehicles, investment in the transport sector, transfers to shareholder personal accounts and large cash withdrawals. It was further observed that the real beneficiaries of the payment were Company R and its Directors. The utilisation of the funds was deemed suspicious.
- vi. It was noted that Company AD was a shell company used to obtain the contract. The award of the contract, its reassignment and payments were all deemed to be irregular.

Based on the above findings, the case was disseminated on possible corrupt practices, fraud and money laundering. The case is under investigation.

Chart 2 illustrates the case study above:

Chart 2: Use of shell companies in public procurement corruption



Case study II: 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 USD43 million to companies KH, ET, SC and SM from 2018 to 2019.

The USD43 million transfer was broken down as below:

- i. Company KH received USD11 million;
- ii. Company ET received USD14.2 million;
- iii. Company SC received USD4 million; and
- iv. Company SM received USD14.4 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's 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.

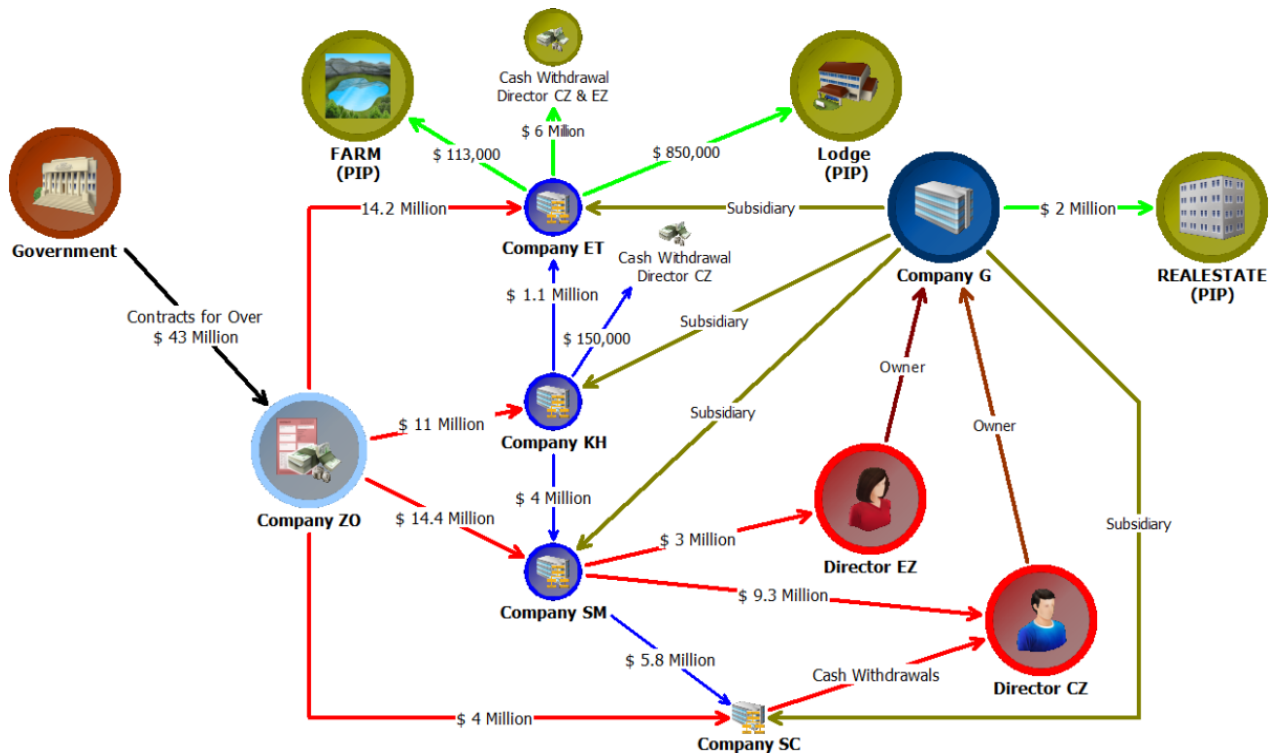
Further analysis revealed that Company ZO received a number of contracts from the Zambian Government.

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.

Chart 3 illustrates the case study above:

Chart 3: Abuse of corporate vehicles for suspected public sector corruption



Case Study III: Abuse of Corporate Vehicles for Suspected Corruption

A foreign owned Company DL was incorporated in February, 2023 and opened a bank account in April, 2023. In June 2023, Company DL was awarded a contract to supply equipment by Government Institution AR. The total contact sum was USD21 million. In August 2023, Company DL received a credit of USD5.6 million in its account from Institution AR as an advance payment.

It was established that Company DL had no previous work experience but had purported to have been involved in works for the construction of a national university when in fact not. A check with the parent Ministry M for Institution AR revealed that the procurement process used was direct bidding and that the solicitation document did not require for previous work experience to be provided by Company DL, which raised a red flag as Company DL was recently incorporated.

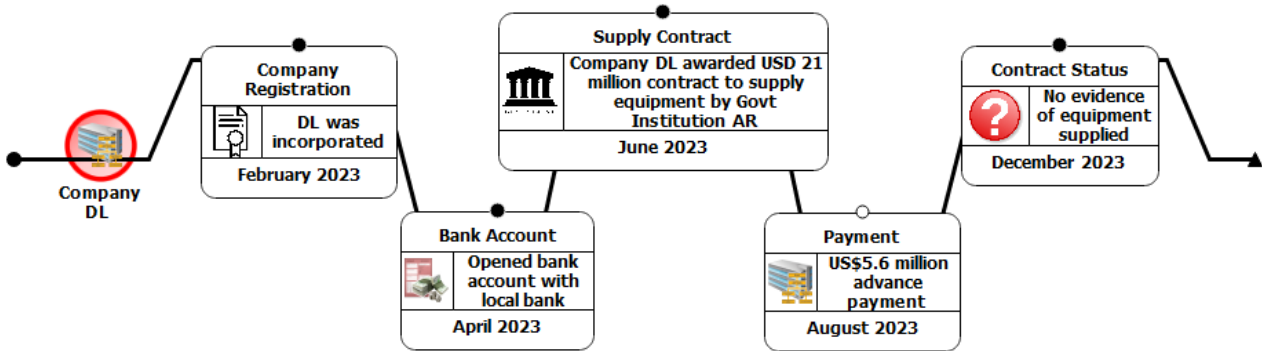
At the time of inquiry there was no evidence that the government equipment had been supplied by Company DL.

At the time of inquiry there was no evidence that the government equipment had been supplied by Company DL

The intelligence report was disseminated to LEAs for investigation on possible corruption.

Chart 4 illustrates the case study:

Chart 4: Abuse of corporate vehicles for suspected corruption



Recommendations on public sector corruption and money laundering:

- i. Government should strengthen the requirement for bidders who participate in public procurement tenders to disclose their beneficial owners;
- ii. Penalties in public procurement corruption cases should be more dissuasive; and
- iii. Government should provide for the debarment of natural persons that are involved in procurement corruption from participating in public tenders.

2.2 USE OF CASH IN ILLICIT TRANSACTIONS

The FIC observed a continuing trend of the use of cash in illicit transactions to obscure the illicit origins of the proceeds of crime. The use of cash to facilitate illicit transactions distances the proceeds of crime from the underlying criminal activities. In this regard, the use of cash in commerce offers a level of anonymity that is attractive to criminals.

Suspicious Transaction Reports and CTRs analysed revealed unusually high cash deposits into corporate bank accounts that were not supported by an underlying revenue generating activity. It was noted that a total of 4,091 STRs were received on cash related transactions in 2023, representing 40% of the total STRs reported. Of these, 381 intelligence reports were disseminated to the Zambia Revenue Authority (ZRA) and the Bank of Zambia (BoZ).

The intelligence reports disseminated to BoZ involved Bureaux de Change owners who were suspected to have enlisted low-income individuals to conduct foreign exchange transactions using their personal accounts. This was done to circumvent foreign exchange currency transaction thresholds and avoid statutory reporting obligations.

The use of cash in illicit transactions continued to be observed in several sectors of the economy, notably the banking, construction, manufacturing, agriculture and in businesses such as legal services and real estate.

The red flags associated with financial crime schemes that involved use of cash in illicit transactions were:

- i. Individuals not linked to any commercial activity depositing large cash transactions;
- ii. Large cash deposits that are immediately transferred out of the country;
- iii. Account holders receive several large deposits from third parties located in different parts of the country inconsistent with their account profiles and immediately withdraw cash equivalent to the amounts deposited; and,
- iv. Individuals insisting to make payment for high value property in cash.

The case studies below illustrate how the schemes involving cash transactions are executed:

Case Study IV: Use of corporate vehicles for suspected money laundering and associated illicit financial flows

The FIC analysed a number of STRs involving over 100 companies that had large cash deposits that were inconsistent with their known profile. The companies held bank accounts at various local commercial banks. Analysis revealed that majority of these companies had Zambian nationals registered as shareholders and beneficial owners. However, the Zambian nationals were being used as ‘strawmen’ and the real beneficial owners were foreign nationals.

It was observed that some companies had used the same physical address as their business address. Further, in some instances, the proprietors of these companies used forged documents to open company bank accounts.

The companies received in excess of USD2.5 billion in the period May 2021 to July 2023. This amount was largely received in form of cash deposits by the

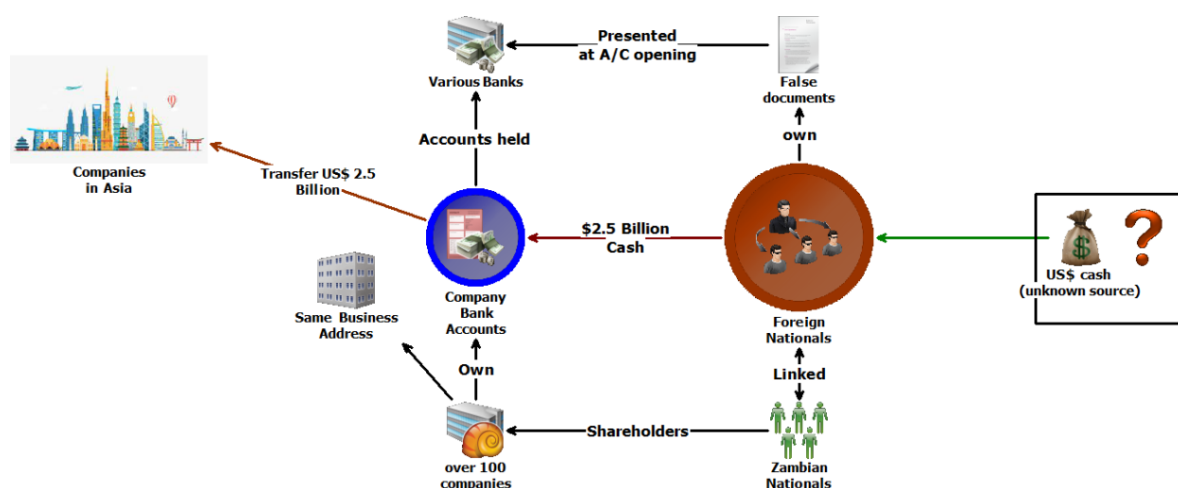
foreign nationals. The source of the cash deposited by the foreign nationals was unknown. The cash deposits were structured to avoid currency transaction reporting thresholds and followed by outward remittances mostly to Asia.

Over the 3-year period, the companies remitted in excess of USD2.5 billion to Asia. The international remittances were mostly for purported purchase of goods; however, they were not supported by any source documents and customs data showed that goods were not imported.

Despite significant income, the companies were either not registered or non-compliant for tax purposes. It was further established that these companies were shell companies.

The intelligence report was disseminated to LEAs for investigation. The chart below illustrates the case study:

Chart 5: Use of corporate vehicles for suspected money laundering and associated Illicit Financial Flows



Case Study V: Use of cash in transactions to conceal fraudulent activities

The FIC analyzed a case of suspected money laundering involving an Accountant VZ at Company XY, who was found to have accumulated property using suspected proceeds of crime. Accountant VZ had credits on his personal bank accounts A and B totalling ZMW6.4 million over the period January 2022 and September 2023. Of the ZMW6.4 million, ZMW3.5 million was made through cash deposits. In the same period Accountant VZ had ZMW2 million worth of transactions on his mobile money Account C.

Analysis of records revealed that Accountant VZ was fraudulently processing cash debits on an account held by Company XY. Further, analysis revealed that he

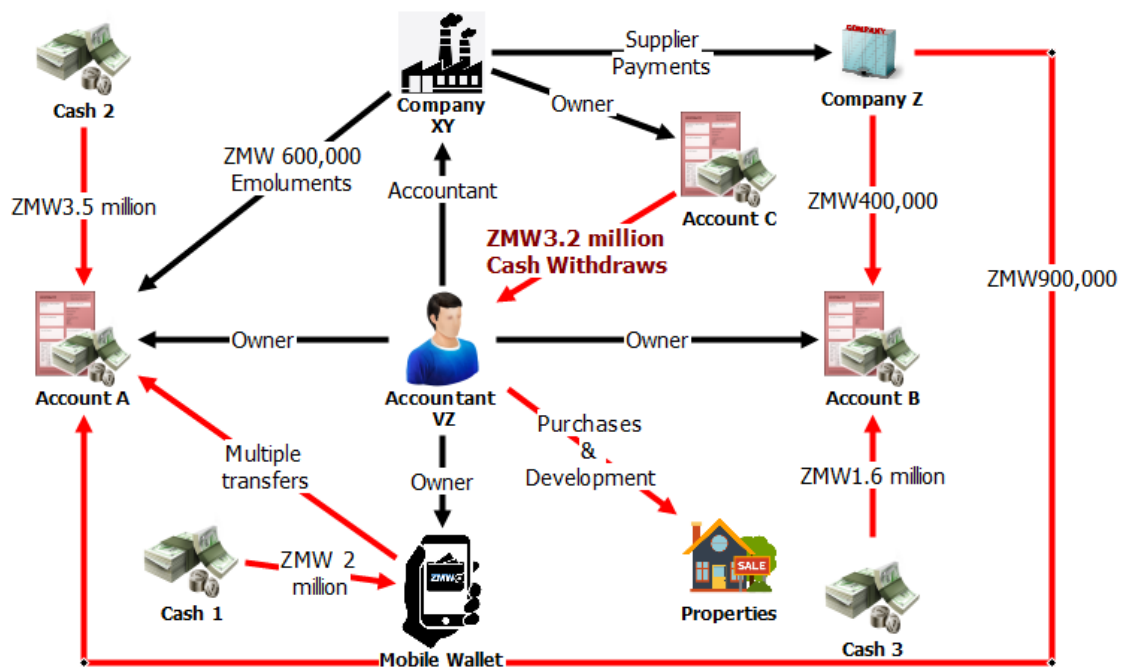
was purporting to process payments to Company Z, a registered supplier of Company XY when in actual fact was making payments to himself.

Analysis of Accountant VZ’s bank accounts revealed transfers to a real estate agent for purchase of properties and a village banking group account. The majority of transfers made by Accountant VZ were indicative of property acquisition and development.

An inquiry on Accountant VZ did not reveal any personal business activity and the only known source of income was his salary from Company XY which was an average of ZMW67,000 per month.

The intelligence report was disseminated to LEAs for investigation. Chart 6 illustrates the case study:

Chart 6: Use of cash in transactions to conceal fraudulent activities



Recommendations on the use of cash in illicit transactions:

- i. The Government should consider limiting the use of cash above certain transactions thresholds; and,
- ii. Consideration should also be given to have a differentiated tax scheme i.e. have lower rates for transactions done electronically.
- iii. Introduction of advance income tax on international remittances for non-tax compliant legal and natural persons.

2.3 MASKING BENEFICIAL OWNERSHIP OF CORPORATE VEHICLES

During the period under review, the FIC observed a continuing trend of masking beneficial ownership information on legal persons and arrangements for purposes of concealing financial crime.

The FIC analysed 450 STRs that were linked to the abuse of legal persons by masking beneficial ownership information. The intelligence reports were subsequently disseminated to the relevant competent authorities. Through its supervision activities the FIC detected 9 legal persons that had not disclosed beneficial ownership information to PACRA as required by the Companies Act.

The FIC has observed that legal persons prone to abuse were operating mainly in the mining, retail and wholesale sectors.

The red flags associated with financial schemes that involve masking beneficial ownership of corporate vehicles were:

- i. Companies with no independent operations, significant assets, ongoing business activity or employees;
- ii. Use of third-parties for shareholding only with no controlling interest;
- iii. Same individuals appearing as shareholders/directors for a number of companies;
- iv. Registering nonfactual information on beneficial owners and business addresses;
- v. Company Bank Accounts denominated by unusually large USD cash deposits;
- vi. Cash deposits made by the same individuals to various companies;

- vii. Externalization of funds for purported purchase of goods with no corresponding imports; and
- viii. Use of multiple accounts to create complex transaction trails.

The case studies below illustrate how schemes involving the masking of beneficial ownership information were executed:

Case study VI: Use of Shell Companies for corruption and money laundering

The FIC analysed an STR on suspected money laundering involving a senior Government official PIP1 who was found to have accumulated government securities in excess of ZMW50 million using suspected proceeds of crime.

Analysis revealed that PIP1 held investment accounts A and B which were largely used for investments in Treasury Bills. Analysis of the said accounts revealed an exponential increase in value of investments from about ZMW300,000 in 2013 to ZMW53 million in 2022. This was mainly due to continuous investments in Government Securities. It was observed that sources of funds were from the following;

- i. Account C (Emoluments): Analysis revealed that in the period 2013 to 2022 the account had a credit turnover of ZMW22 million from salaries, subsistence allowances, loans and retirement. It was revealed that ZMW11 million of the said funds were transferred to investments accounts A and B over the analysis period.

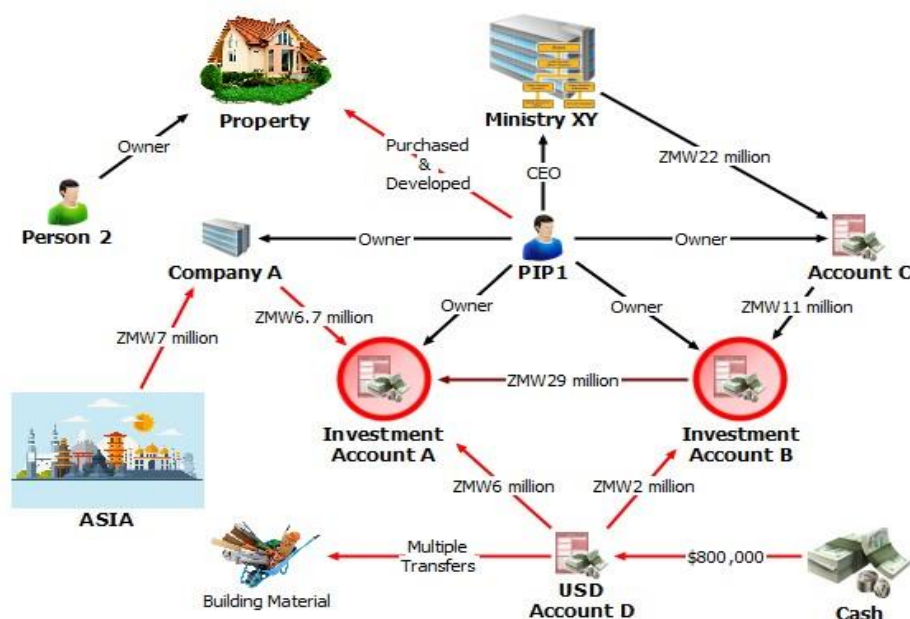
- ii. USD Account D: Analysis revealed that from 2013 to 2022, the account received in excess of USD800,000 in cash deposits sometimes on a daily basis in structured amounts below USD5,000. Debits on the account were transfers to investment accounts A and B and outward wire transfers were noted mainly to a country in Southern Africa for the purchase of building material, household furniture, among other transactions.

- iii. Company A: Analysis revealed that company A was owned by PIP1 and his brother. Analysis revealed that Company A held a bank account that was only active between 2014 and 2015. The only credits on the accounts were wire transfers from two companies in China totalling ZMW7 million. Most of the said funds were transferred to investment account A and added to the Treasury Bills portfolio. It was established that company A was a shell company with no business activity and may have been created for the sole purpose of receiving funds from Asia.

Transactions by PIP1 were suspicious as they were over and above his official government income. Analysis revealed that legitimate funds were comingled with suspected proceeds of crime in Account D and from Company A to build a large portfolio of Government Securities. Further, PIP1 had acquired and developed high value property but maintained the property in the previous owners' names since 2014, indicating concealment of suspected proceeds of crime.

The intelligence report was disseminated to LEAs for investigation. Chart 7 illustrates the case study:

Chart 7: Use of shell companies for corruption and money laundering



Case study VII: Abuse of Corporate Vehicle in Ponzi Scheme

The FIC analysed a STR in which Company Q was running a ponzi scheme. Individuals C, D and T were the shareholders of Company Q. The company was advertising various investment schemes on their website and other social media platforms. The investment products were being advertised for a minimum investment amount with a promise of high returns depending on the initial investment.

Analysis of Company Q revealed that one of its shareholders was also a shareholder in Company T which was under investigation by LEAs for running a similar ponzi scheme.

Over a period of one year, Company Q's bank account

B had been credited with funds in excess of ZMW 35 million. These were cash deposits by unsuspecting members of the public. The narrations on these deposits indicated that they were payment for various investment products.

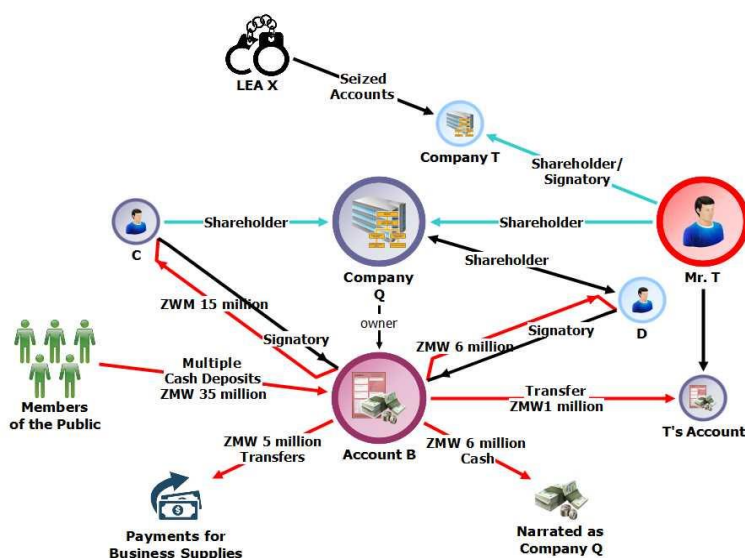
Analysis of Company Q's bank account B revealed that:

- Shareholder C received a transfer of ZMW15 million
- Shareholder D received a transfer of ZMW 6 million
- Shareholder T received a transfer of ZMW1 million

Further it was noted that shareholder C and D were signatories of Company Q's account. The intelligence report was disseminated to LEAs for investigation.

The chart below illustrates the case study above:

Chart 8: Abuse of corporate vehicles in ponzi



Recommendations on masking beneficial ownership of corporate vehicles

The Government should adopt an “All Government approach” for disclosure of beneficial ownership information by legal persons and arrangements, including;

- Requiring legal persons and arrangements to disclose their beneficial ownership information when accessing Government services such as licencing, tax registration, social security scheme registration, building permits, title to lease hold land, electricity connection, water connection, motor vehicle registration, empowerment loans and contracts under the constituency development fund;

- Requiring all corporate vehicles bidding for public procurement contracts to be subject to enhanced beneficial ownership verification procedures. These enhanced verification procedures will require a corporate vehicle to engage an accredited profession such as a legal practitioner or accountant to verify the veracity of the beneficial ownership information disclosed by the corporate vehicle;
- Enhance more awareness on the concept of beneficial ownership among stakeholders; and
- Competent authorities should enhance awareness among the public on ponzi scheme structured as investment products.

2.4 CYBER ENABLED FINANCIAL CRIMES

The FIC observed an increase in cyber enabled financial crimes particularly targeted at the financial services sector. Cyber enabled crimes have been appearing in the FIC's trends reports as an emerging crime since 2014. It has been observed that the majority of the cyber enabled financial crimes were perpetrated by individuals from East Africa working with Zambian nationals. With increased automation, interconnectedness and reliance on electronic payment platforms, cyber enabled financial crimes have been on the rise.

Majority of the cyber enabled financial crimes were perpetrated by individuals from East Africa working with Zambian nationals

The red flags associated with the cyber enabled financial crimes include:

- i. The use of fraudulent documents to open and operate bank accounts;
- ii. Large fund transfers followed by immediate ATM withdrawals and POS transactions;
- iii. Duplication of cards in order to access accounts;
- iv. Individuals holding multiple e-wallets in different names for the purposes of structuring transactions;
- v. E-wallet enabled fraudulent activities on the public through social engineering.

The case studies below illustrate how schemes involving cyber enabled financial crimes were executed:

Case Study VIII: Cyber enabled fraud involving a foreign jurisdiction

The FIC received an alert when a person in a foreign jurisdiction was defrauded of USD210,000 through cyber enabled fraud. The funds had been transferred to Company X's bank account held with a Zambian financial institution.

The FIC issued a freezing order on Company X's US dollar bank account. Analysis of the bank account revealed that Company X had received cash deposits in excess of USD 15 million. The source of the cash deposit was unclear. The cash deposits were comingled with the funds from the fraud incident.

Additionally, analysis revealed that the Company X's shareholders, directors and beneficial owners were foreign nationals (Asian origin) and they did not have valid permits to operate in Zambia.

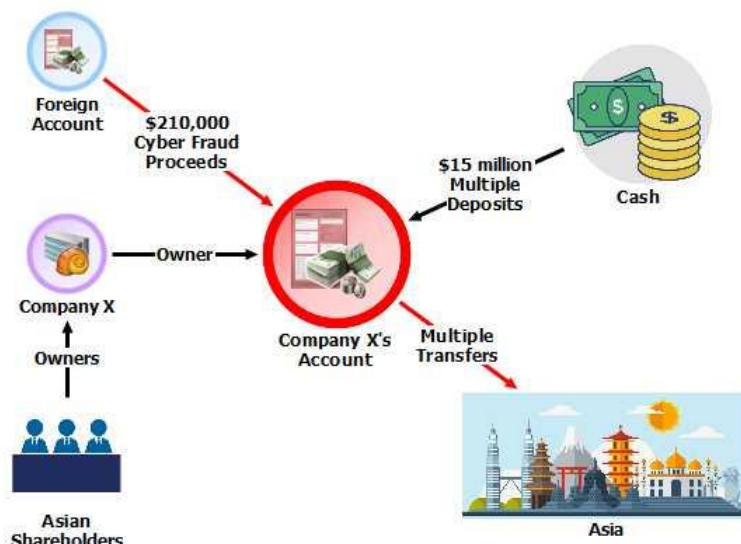
Further, analysis revealed that false information was provided during company registration at PACRA as evidenced by a mismatch in the registered business activities and actual income generating activities

The FIC also observed that Company X would make remittances to Asia for purchase of goods, however there was no evidence of receipt of the physical goods.

The intelligence report was disseminated to LEAs for investigations.

Chart 9 illustrates the case study:

Chart 9: Cyber enabled fraud involving a foreign jurisdiction



Case Study IX: Cyber enabled fraud on multiple financial institution

The FIC collaborated with a multi-agency investigation team after a syndicate of cyber attackers gained access to the customer accounts of four (4) financial institutions and transferred huge sums of money to several beneficiary accounts.

The syndicate suspected to have originated from East Africa enlisted Zambian nationals to open bank accounts and mobile money wallets using both authentic and counterfeit documents. The Zambian nationals were incentivised by token payments ranging from ZMW 3,000.00 to ZMW 20,000.00, to provide their personal information and access to their accounts.

Once these accounts were established, the SIM cards and bank VISA cards associated with them were handed over to the recruiters. In addition, insiders within

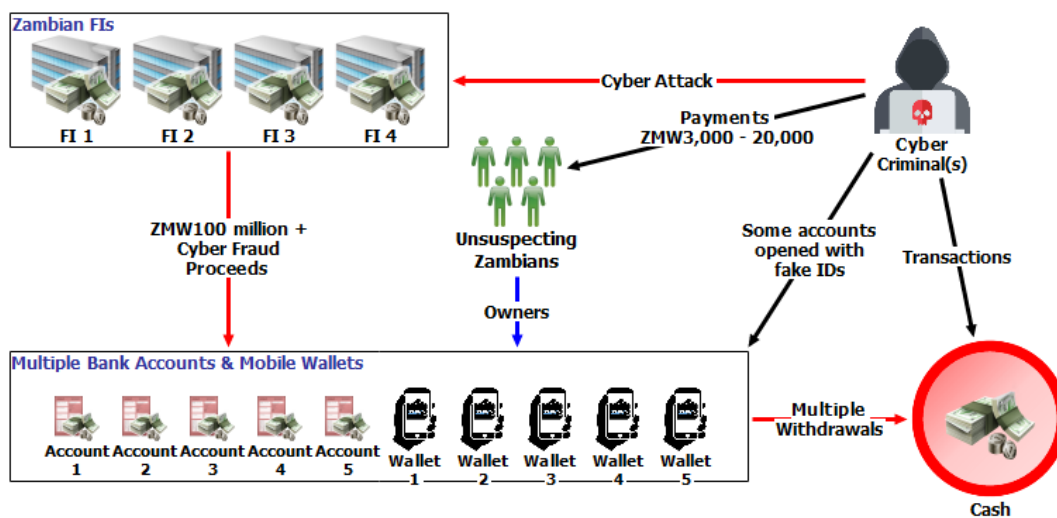
financial institutions and MVTs were recruited. Through the insiders, malware was introduced which allowed the subjects to gain unauthorized access to the financial institution's systems and subsequent fraudulent transfers.

The hackers accessed the fraudulent funds using various platforms locally through utilizing mobile money wallets and VISA cards to conduct international transactions and cash withdrawals. This multi-faceted approach allowed the subjects to move funds quickly and efficiently leading to the loss of funds in excess of ZMW100 million.

The inquiry revealed that the same individuals were responsible for all the attacks on the 4 financial institutions. The case has proceeded to court.

The chart below illustrates the case study above:

Chart 10: Cyber enabled fraud on multiple financial institutions



Recommendations on cyber enabled financial crimes:

- i. Strengthen transaction monitoring systems within mobile money service providers to detect anomalous transaction patterns;
- ii. Increased consumer awareness on cyber enabled financial crimes;
- iii. Implementation of the biometric identification system; and
- iv. Sensitisation of the public on e-wallet enabled fraud schemes including transaction prompts reminding customers of fraud risks.

2.5 ABUSE OF CASINOS FOR MONEY LAUNDERING

During the period under review, the FIC observed an increasing trend of abuse of the casino sector for money laundering and other nefarious activities. The following trends were observed;

- i. High usage of cash in casino operations; this operating model was being used to facilitate the payment of bribes and avoid creation of a transaction audit trail. Further, the lack of a transaction audit trail was used by proprietors of these casinos to under declare income;
- ii. Some casinos were offering prostitution services to their patrons. The funds generated from were commingled with legitimate casino earnings;
- iii. Proprietors of casinos were registering their Zambian workers (e.g. cleaners, home helpers, receptionists, and gardeners) as legal owners of the casino enterprise. This was a scheme to mask beneficial ownership of the casino. Further, it was observed that majority of Casinos had not disclosed their beneficial owners to the Patents and Companies Registration Agency as required. However, it was observed that payments made to Prominent Influential Persons (PIP) suggested that they may have had an interest in the sector;
- iv. Some casinos were involved in illegal cross border transportation of cash; and
- v. Financial institutions were de-risking casinos, consequently casinos began to hide their real identity behind false business names to access the financial system.

The red flags associated with abuse of casinos for illicit transactions are:

- i. Masking of beneficial owners;
- ii. High use of cash in all transactions; and
- iii. Non-maintenance of customer records.

The case study below illustrates how schemes involving abuse of casino business were executed:

Case study X: Use of casino premises for illegal money lending business

The FIC analysed a STR on Casino ZC owned by a foreign company and a local company. Casino ZC had a money lending Company DC operating within its premises. Company DC was owned by Shareholder XT and VF. Shareholder XT and VF were foreign nationals based in Zambia. Analysis revealed that Casino ZC and Company DC had not declared their beneficial owners with the Patents and Companies Registration Agency. Shareholder XT and VF were on a residence permit and

employment permit respectively. Though Shareholder VF had incorporated Company DC his employment permit did not allow for him to incorporate a company.

Verifications conducted revealed that Company DC was providing illegal money lending services to patrons of Casino ZC. Company DC would provide the loans in the form of casino chips/tokens. Inquiries established that Shareholder VF was receiving large credit transactions on his personal account. The large credits received would then be lent out to patrons of Casino ZC using casino chips/tokens. The source of the credits on Shareholder VF's account was unknown. A check with the licensing authorities revealed that Company DC did not have a money lenders license.

In the period January to July 2022, Shareholder VF had undertaken cash-in and cash-out transactions in Casino ZC worth over ZMW150 million. It was suspected that the cash-in and cash-out transactions were in connection with the illegal money lending business that was done in Casino ZC. Furthermore, it was suspected that Shareholder VF operating under Company DC was using Casino ZC to launder funds using point-of-sale transactions performed in the Casino ZC.


Analysis of the bank accounts of Shareholder XT and VF revealed a large number of transactions connected to Casino ZC. Further, analysis of the transactions revealed that these personal bank accounts were being used to account for some of the money lending business transactions. Company DC did not have a bank account and was not registered for tax purposes.

Intelligence gathered was that Casino ZC was also offering foreign currency changing services to its patrons without a license. The intelligence report was disseminated to relevant competent authorities for investigation.

Recommendations on abuse of casino sector for money laundering:

Strengthen the casino regulatory regime including;

- i. Vetting applicant procedures including preventing suspected criminals and their associates from holding an interest;
- ii. Increasing licensing and application fees and capital requirements so as to deter the proliferation of casinos;
- iii. Setting up a government agency mandated with the prudential and AML/CFT supervision of the casinos and gaming sector.



CHAPTER 3:
COMPLIANCE BAROMETER
AND AWARENESS

3.1 COMPLIANCE BAROMETER

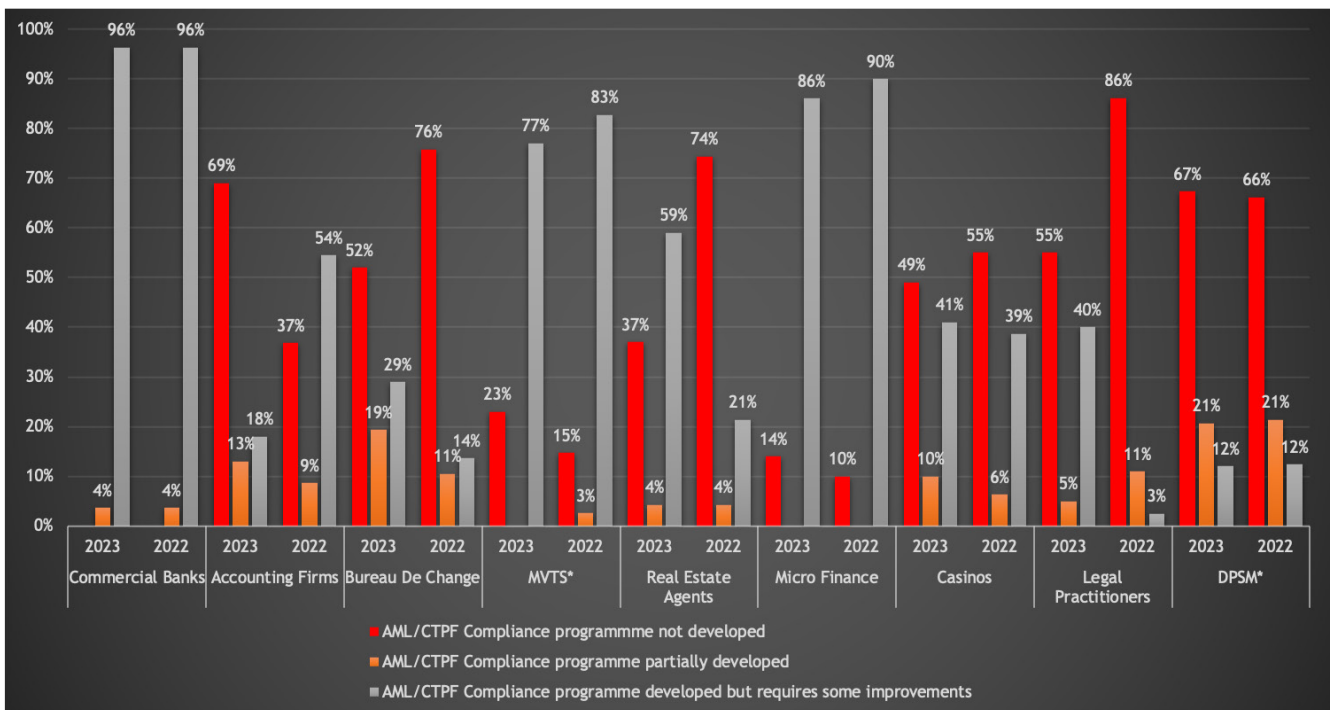
The compliance barometer provides a snap-shot of the status of AML/CFTP compliance programmes in the sectors supervised by the FIC. It further measures the sectors’ technical compliance to the requirements of the FIC Act but is not indicative of the effectiveness of the implementation of the compliance requirements by reporting entities.

The compliance barometer shows that the banking sector still remains with the highest levels of technical compliance with AML/CFT requirements, with only 4 percent of the sector assessed as having partially developed the compliance Programme. The FIC observed improvements in levels of technical compliance by law firms and real estate agents in 2023 compared to 2022.

The compliance barometer provides a snap-shot of the status of AML/CFTP compliance programmes in the sectors supervised by the FIC

The banking sector still remains with the highest levels of technical compliance with AML/CFT requirements

Chart 11: Compliance Barometer



Bureaux De Change and Casinos also showed some level of improvements in their AML/CFT compliance programme in 2023 compared to 2022. The accounting and audit firms showed lower levels of technical compliance in 2023 compared to 2022. However, this was largely attributable to the FIC having undertaken monitoring of accounting firms in 2023 that had never been monitored before for AML/CFT purposes.

The FIC in collaboration with other supervisory authorities plans to intensify supervision activities in those sectors where compliance levels are low. It is envisaged that these joint supervision activities will facilitate skills transfer between supervisory authorities. Further, the FIC Act will be reviewed to allow for more dissuasive administrative sanctions for non-compliance to AML/CFT requirements.

The FIC in collaboration with other supervisory authorities plans to intensify supervision activities in those sectors where compliance levels are low

The FIC had several media engagements which included featuring on radio and television programs.

3.2 AWARENESS AND TRAINING

3.2.1 Education and Awareness Activities

The FIC carried out awareness activities for various stakeholders in the private and public sectors to increase awareness on the FIC's mandate and to educate reporting entities and accountable institutions on their obligations under the FIC Act.

FIC Act will be reviewed to allow for more dissuasive administration sanctions for non-compliance to AML/CFT requirements

In the period under review, the FIC conducted awareness sessions for a total of 1,574 participants compared to 1,704 participants in 2022. Stakeholders engaged were from the following sectors; virtual asset service providers, motor vehicle dealers, travel agents, real estate, insurance, casinos, Money or Value Transfer Service (MVTs) providers and financial institutions.

FIC conducted awareness sessions for a total of 1,574 participants compared in 2023 to 1,704 participants in 2022

The FIC provided a series of specific training sessions for legal practitioners in conjunction with the Law Association of Zambia (LAZ). Further, the FIC collaborated with the National Anti-Terrorism Centre (NATC) to conduct joint countrywide awareness sessions with government agencies and financial institutions on Terrorism and Proliferation Financing threats.

During the period under review, the FIC had several media engagements which included featuring on radio and television programs.

In 2023 the FIC updated and published ten (10) sector specific guidelines in collaboration with various supervisory authorities.

3.2.2 Designation of Compliance Officers

Approximately 154 Compliance Officers of reporting entities were approved by the FIC in 2023. The majority of compliance officers (37%) vetted and approved by the FIC in 2023 were appointed in the 3rd quarter. This was due to collaboration with and measures introduced by the Pensions and Insurance Authority (PIA) who tied the renewal of annual licenses by their regulated entities to the approval of compliance officers by the FIC. This measure is being extended to other sectors.

Approximately 154 Compliance Officers of reporting entities were approved by the FIC in 2023

3.2.3 National AML/CFTP Policy

In line with international standards and as informed by the domestic Money Laundering (ML)/Terrorist Financing (TF)/Proliferation Financing (PF) risk context, Zambia developed and published its first ever National Anti-Money Laundering/Countering Terrorism and Proliferation Financing ((AML/CTPF) Policy which was launched by the Attorney General on 2nd February, 2023. This was a clear demonstration of the political leadership and commitment to fighting ML/TF/PF, associated financial and economic crimes in Zambia.

Zambia developed and published its first ever National Anti-Money Laundering/Countering Terrorism and Proliferation Financing ((AML/CTPF) Policy

The National AML/CTPF Policy provides a framework within which ML, TF, PF and associated predicate crimes will be effectively addressed. The overarching objective of this Policy is to effectively fight ML/TF/

PF crimes in Zambia. The FIC collaborated with MoFNP in distributing the National AML/CFT Policy to all the provinces.

The overarching objective of this National AML/CTPF Policy is to effectively fight ML/TF/PF crimes in Zambia

3.2.4 Second Money Laundering/Terrorist Financing/Proliferation Financing National Risk Assessment

In the third quarter of 2023, Government approved the Cabinet Memorandum for Zambia to undertake the 2nd round Money Laundering (ML)/Terrorism Financing (TF) /Proliferation Financing (PF) National Risk Assessment (NRA) which is scheduled for completion in December 2024.

Government approved the Cabinet Memorandum for Zambia to undertake the 2nd round ML/TF/PF National Risk Assessment (NRA)

The FIC was designated to coordinate the undertaking of the second round NRA. The NRA among others will cover legal persons and arrangements, virtual asset service providers, environmental crimes (wild life, forestry and mining) and proliferation financing.



CHAPTER 4:
STATISTICS

4.1 SOURCES OF INFORMATION

The FIC receives reports from reporting entities and competent authorities pursuant to sections 26, 29, 30 and 38 of the FIC Act. Section 29 and 30 of the FIC Act No. 46 of 2010 (as amended) requires reporting entities to submit Suspicious Transaction Reports (STRs) and Currency Transaction Reports (CTRs), respectively.

In addition, Section 38 of the FIC Act as read with Regulation 8 of the FIC (Prescribed Threshold) Regulations, 2022; the FIC receives Cross Border Currency Declaration Reports (CBCDRs) from the Zambia Revenue Authority. The Bank of Zambia provides the FIC

with wire transfer records pursuant to Section 26 of the FIC Act.

Suspicious Transaction Reports (STRs) are submitted on suspected or attempted money laundering, financing of terrorism or proliferation financing or any other serious offence.

Currency Transaction Reports (CTRs) 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.

Table 4.1: Number of reports received over a 3-year period

Year	Number of reports received		
	2023	2022	2021
STRs	10,293	5,745	2,577
SDR	78	62	43
CTRs	285,004	239,717	145,852
CBCDRs	3,421	4,025	1,720

Source: Financial Intelligence Centre, Zambia 2023

Cross Border Currency Declaration Reports (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.

The FIC also receives spontaneous disclosures 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 4.1 shows the number of reports received over a period of 3 years.

4.1.1 Suspicious Transactions Reports Received

In 2023, the FIC received a total of 10,293 STRs compared to 5,745 in 2022 representing an increase of 78.97 percent. The significant increase was attributed to the FIC's heightened supervision activities such as awareness training, inspections and enforcement actions.

In addition, there were specific cases where reporting entities had been found not to have reported some STRs and were directed by the FIC to submit the backlog of unreported STRs. The value of reports received in 2023 was ZMW 11.36 billion while the value of reports received in 2022 was ZMW 5.97 billion, representing an increase of ZMW 5.39 billion.

In 2023, the FIC received a total of 10,293 STRs compared to 5,745 in 2022 representing an increase of 78.97 percent

The reasons for suspicion that were most prevalent in the STRs received in 2023 were on account of large or unusual cash deposits and withdrawals, large inward and outward remittances, activity inconsistent with customer profile and unusually large foreign currency transactions. The 2023 trends with regard to reasons for suspicion were similar to those observed in 2022 and 2021.

Table 4.2: STRs received by number and value over a 3-year period

Year	2023	2022	2021
Number of reports	10,293	5,745	2,577
Value in millions (ZMW)	11,364	5,970	6,533

Source: Financial Intelligence Centre, Zambia 2023

The continuing trends on large or unusual cash deposits and withdrawals was prevalent because of the high usage of cash in the economy and the level of anonymity that cash transactions provide. These unusual cash deposits and withdrawals were denominated both in Kwacha and foreign currencies such as United States Dollar and Euro.

Unusual cash [transactions] were prevalent because of the high usage of cash and level of anonymity that cash transactions provide in the economy

In some cases, customers made unusual large cash deposits which were inconsistent with their profile and immediately instructed the financial institution to transfer the funds to foreign jurisdictions.

4.1.2 Suspicious Transaction Report received by Sector

In 2023, the banking sector continued to be the highest reporting sector of STRs with 98 percent of the filling. The banking sector has maintained a year-on-year increase of over 100 percent in the number of STRs submitted to the FIC in the last 3 years. The significant increase was attributed to heightened supervision activities by the Bank of Zambia and FIC.

Further, improvements in the AML/CFT infrastructure deployed by the banking sector also contributed to the increase in STRs submitted. The Mobile money service providers (MMSP) accounted for the second highest source of STRs after the banking sector. The number of STRs reported in 2023 by the MMSP was 163 compared to 144 in 2022.

The Mobile money service providers (MMSP) accounted for the second highest source of STRs after the banking sector

The FIC observed a reduction in the number of STRs received from the DNFBPs sector from 15 reports in 2022 to none reported in 2023. The low number of STRs received from the DNFBP sector over the last 3 years was attributed to lack of expertise and investment in AML/CFT systems by reporting entities in the sector.

The FIC observed a reduction in the number of STRs received from the DNFBPs sector from 15 in 2022 to none in 2023.

In addition, the sector has historically not been subject to this level of regulation and as a result this has impacted its rate of growth with regard to AML/CFT compliance. In addition to increasing awareness activities in the sector, the FIC also commenced the imposition of administrative sanctions on non-compliant reporting entities.

FIC also commenced the imposition of administrative sanctions on non-compliant reporting entities

The MVTS and Microfinance subsectors have exhibited a steady rise in the number of STRs submitted to the FIC year-on-year over the last 3 years. This is attributed to increased levels of awareness in the sectors and investment in expertise. There was a significant drop in the number of reports received from the casino sector in 2023 compared to 2022. This is attributable to low levels of AML/CFT knowledge in the sector and its vulnerability to abuse for ML.

Table 4.3: Number of STRs received by sector

Sector	Number of reports received by sector over a 3-year period		
	2023	2022	2021
Commercial banks	10,072	5,574	2,522
MVTS Providers	163	144	42
Microfinance	43	8	13
Casinos	0	15	0
Accounting firms	0	2	0
Law firms	0	0	0
Insurance	4	0	0
Bureau de Change	0	0	0
Virtual Asset Service Provider	11	0	0
Motor vehicle dealers	0	2	0
Total	10,293	5,745	2,577

Source: Financial Intelligence Centre, Zambia 2023

In 2020, the FIC Act was amended to introduce provisions that would require Virtual Asset Service Providers (VASPs) to implement AML/CFTP measures. As a consequence, VASPs were designated as reporting entities by the FIC Act and subject to AML/CFTP regulation by the FIC.

VASPs are designated as reporting entities by the FIC Act and subject to AML/CFTP regulation by the FIC

Further, the FIC Act requires all VASPs operating in Zambia to be registered with the FIC.

The FIC Act defines VASPs as any person who as a business conducts one or more of the following activities or operations for or on behalf of another person:

- exchange between virtual assets¹ and fiat currencies;
- exchange between one or more forms of virtual assets;
- transfer of virtual assets;
- safekeeping and administration of virtual assets instruments enabling control over virtual assets;

- participation in and provision of financial services related to an issuer's offer and sale of a virtual asset; and,
- provision of intermediary services for the buying and selling of virtual assets, including through the use of virtual asset vending machine facilities.

As at December 2023, the FIC had registered three (3) VASPs operating in Zambia. Further, there were eleven (11) STRs received from VASPs in 2023.

4.1.3 Suspicious Transaction Reports Analysed

A total number of 15,696 STRs were analysed in 2023 compared to 155 STRs analysed in 2022. The significant increase in the number of STRs analysed in 2023 was attributed to a special exercise undertaken by the FIC in the fourth quarter of 2023. The exercise was aimed at reducing the back-log of STRs and support the identification of sectors of high-risk concentration.

The number of STRs analysed in 2023 was attributed to a special exercise undertaken by the FIC in the fourth quarter of 2023

¹ Virtual asset means convertible virtual asset such as crypto currency or other digital means of exchange where the virtual asset is accepted by a person as a means payment for goods or services, a unit of account, a store of value or a commodity

The exercise revealed a pattern of suspected tax evasion, forgery and/or money laundering involving foreign nationals who were engaged in the transfer of suspected illicit funds out of Zambia. The schemes involved the abuse of corporate vehicles through masking of beneficial owners. The corporate vehicles were either registered for incorrect tax types or not registered at all. The illicit funds were introduced into the financial system mainly through large cash deposits made in US Dollars.

The exercise revealed a pattern of suspected tax evasion, forgery and/or money laundering involving foreign nationals

These funds were then transferred out of the country on the pretext of paying for imports with no evidence of corresponding goods received by the importer. Further analysis revealed that sectors with a high-risk concentration were mining, retail and wholesale.

4.1.4 Intelligence Reports Disseminated

During the period under review, the FIC disseminated a total of 923 reports to Law Enforcement Agencies (LEAs) compared to 129 in 2022, representing a 133 percent increase while the values attributed to the disseminations also increased to ZMW 13.58 billion in 2023 from ZMW 5.83 billion in 2022.

The FIC disseminated a total of 923 reports to Law Enforcement Agencies (LEAs) compared to 129 in 2022

The increase in the number of disseminations was as a result of a special exercise undertaken by the FIC. In 2023, the FIC closed 14,733 reports received for lack of merit. Table 4.4 below provides a comparison of disseminations over a 3-year period:

Table 4.4: Intelligence Reports disseminated

Suspected Offence	2023	2022	2021
	Number	Number	Number
Corruption	9	10	4
Fraud	6	4	3
Money laundering	11	44	16
Tax evasion	450*	52	17
Terrorism financing	0	11	4
Violations (BFSA SI No. 38, 2003)	443	8	0
Violation of Immigration and Deportation Act	4	0	0
Grand total	923	129	44

Source: Financial Intelligence Centre, Zambia 2023

*These disseminations were done in December 2023.

4.1.5 Feedback on Disseminated Intelligence Reports

During the period under review, the FIC received feedback from Competent Authorities on the intelligence reports disseminated. The feedback received from competent

authorities in some cases may include cases that were disseminated in previous years.

The table below provides the status of cases disseminated to LEAs:

Table 4.5: Status of cases disseminated

Institution	Status	No. of Cases
Drug Enforcement Commission	Suspects undetected	11
	Transferred to other LEAs	10
	Nolle Prosequi	3
	Arrested	4
	Convicted	1
	In court	5
	Acquittal	1
Anti-Corruption Commission	Investigations ongoing	48
	Transferred to other LEAs	7
	In court	7
	Closed	1
National Anti-Terrorism Centre	3 under investigation	3
	1 case was closed	1
Zambia Revenue Authority	Tax assessments amounting to ZMW 1.2 billion in principal tax, interest, and penalties. Recoveries of ZMW 3,534,773.91 were made.	

Source: Financial Intelligence Centre, Zambia 2023

Most of the disseminations went to the ZRA on the account of the high levels of illicit financial flows associated with tax evasion. As at the close of 2023, the ZRA had assessed ZMW1.2 billion worth of taxes on income that was previously undetected.

Feedback received from other LEAs on disseminated reports indicated that the cases were at investigation and prosecution stages. Further, accused persons were convicted in some cases, while non-conviction based forfeitures were recorded in others.

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 (15) days.

The effect of Section 10(3), is that on receipt of the Freezing or Suspension Order a reporting entity must for the period of time specified in that order stop all activities or suspend a specified transaction on the concerned account with the exception of credits being received into that account.

However, it must be noted that the minimum requisite conditions for the FIC to exercise this power to either freeze an account or suspend a transaction is that the Director General must reasonably suspect that a transaction relates to money laundering, financing of terrorism or proliferation.

It is noteworthy that the freezing of an account or suspension of a transaction is not absolute. Section 10(4) outlines the process for challenging the Director General's decision to freeze an account or suspend a transaction. It allows an aggrieved party after seventy-two (72) hours of the Director General placing an order to freeze an account or suspend a transaction apply to a Judge in Chambers to have it discharged and at the

same time serve a Notice on the Director General to join the proceedings. Notwithstanding the legal recourse being sought by an aggrieved party through the already explained application to a Judge in Chambers, the Freezing or Suspension Order remains in effect until the Judge determines otherwise.

Pursuant to section 10(3) of the FIC Act, the FIC issued 27 freezing orders on 27 commercial bank accounts with a cumulative account balance of USD 2.8 million and ZMW 126.5 million in 2023. The basis for the freezing orders were suspected money laundering. Further, the FIC had issued 3 freezing orders for 3 commercial bank accounts with a cumulative account balance of ZMW 31.1 million in 2022. The freezing orders are issued to facilitate investigations by law enforcement agencies.

4.2 CURRENCY TRANSACTION REPORTS

4.2.1 Currency Transaction Reports Received

In 2023, the FIC observed an 18.8 percent increase in the number of CTRs received. In absolute terms, the number of CTRs had increased to 285,004 CTRs in 2023 from 239,717 in 2022. The value of CTRs increased to ZMW501.66 billion in 2023 from ZMW379.69 billion in 2022. The increase in the number and value of CTRs is a continuing trend that has been observed in previous years.

Given the high availability of multiple electronic payment platforms in the economy, it would be expected that the number and value of cash transactions in the economy would trend downwards. However, through its analysis work the FIC has observed that cash transactions remain attractive in the economy because of the anonymity it provides.



Analysis of the STRs received revealed that majority had reasons for suspicion based on large cash transactions that were inconsistent with the customer’s profile. In some cases, customers would make large cash deposits that were not within their known profile and immediately instruct the financial institution to transfer the money to a foreign jurisdiction.

Analysis according to provinces revealed that Lusaka province had the highest transactions in terms of number and value, followed by the Copperbelt province. A number of these reports were found to be linked to suspected IFFs and foreign exchange trading in the border areas such as Kasumbalesa.

Table 4.6: Number of CTRs received from 2021 to 2023

Year	Number of CTRs
2023	285,004
2022	239,717
2021	145,852

Source: Financial Intelligence Centre, Zambia 2023

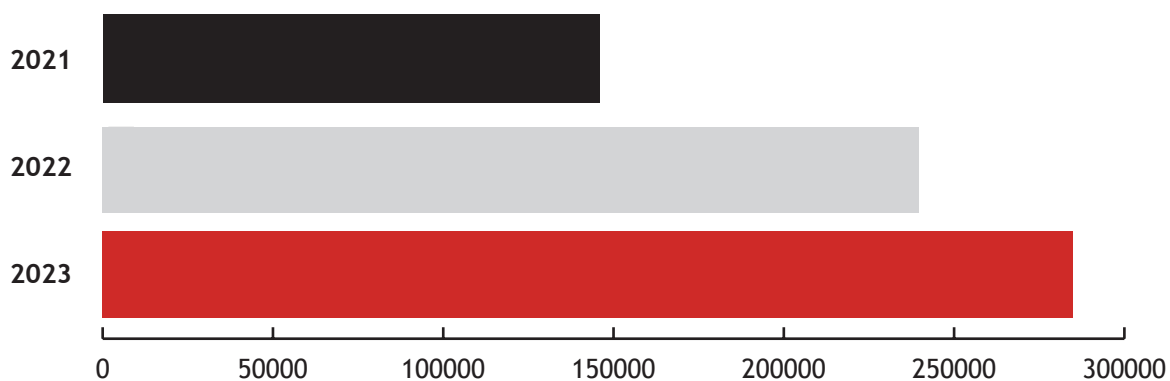


Chart 12: Number of CTRs over a 3-year period

Table 4.7: Corporate CTRs by province

Province	Number of Transactions			
	Q1	Q2	Q3	Q4
Lusaka	28,294	32,770	38,449	28,750
Copperbelt	7,040	9,541	10,224	8,337
Eastern	1,062	1,477	1,747	1,207
Southern	1,009	1,307	1,731	1,174
Central	926	1,390	1,506	1,130
Luapula	230	231	276	189
North Western	390	398	475	368
Muchinga	278	439	405	231
Western	156	249	225	148
Northern	114	196	321	186
Unclassified	236	0	478	315
Total	39,735	47,998	55,837	42,035

Source: Financial Intelligence Centre, Zambia 2023

Table 4.8: Individual CTRs by province

Province	Number of Transactions			
	Q1	Q2	Q3	Q4
Lusaka	10,193	13,665	16,486	11,140
Copperbelt	5,942	4,882	5,979	4,868
Eastern	1,305	1,602	2,486	1,401
Muchinga	1,032	864	711	556
Southern	798	1,161	2,345	872
Central	579	1,075	1,552	752
Northern	246	260	398	266
North Western	226	314	462	372
Western	180	272	272	235
Luapula	100	135	130	106
Unclassified	2,440	0	347	352
Total	23,041	24,230	31,168	20,920

Source: Financial Intelligence Centre, Zambia 2023

4.3 CROSS BORDER CURRENCY DECLARATION REPORTS

In the period under review, the FIC received 3,421 CBCDRs with a total value of USD 642.83 million compared to 4,025 CBCDRs with a total value of USD 1.08 billion in 2022. The declarations in 2023 were made by travelers

from 44 nationalities. The top 10 nationalities with the highest aggregate value of declarations in the period are as shown Table 4.9:

Table 4.9: Top 10 nationalities with the highest value of declarations

Nationalities	Frequency of Declaration	Aggregate Value of Declarations (USD'million)
Democratic Republic of Congo	2541	379.05
Congo Brazzaville	389	248.20
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

Source: Financial Intelligence Centre, Zambia 2023

In terms of the ports of entry with the highest value of declarations, Kasumbalesa Border Post had the highest value in 2023 with USD 416 million. This could be a reflection of the value of trade between Zambia and

the Democratic Republic of Congo. The table below shows declarations at various ports of entry into the country.

Table 4.10: Aggregate value of declaration based on ports of entry

Borders/Ports of Entry	Aggregate value of declarations (USD' million)
Chirundu	0.21
Kariba	0.02
Kasumbalesa	416.08
Kazungula	0.035
Lusaka International Airport	13.27
Lufuwa	0.014
Mukambo	16.66
Mwami	0.033
Ndola International Airport	0.47
Nakonde	0.046
Sakania	196
Victoria Falls	0.038
Total	642.00

Source: Financial Intelligence Centre, Zambia 2023

NOTES





ANNEX:
WORKING DEFINITIONS

COMPETENT AUTHORITY: Refers to all public authorities with designated responsibilities for combating money laundering and/or terrorist financing. In particular, this includes the FIU:

- authorities that have the function of investigating and/or prosecuting money laundering, associated predicate offences and terrorist financing, and seizing/freezing and confiscating criminal assets;
- authorities receiving reports on cross-border transportation of currency & BNIs; and,
- authorities that have AML/CFT supervisory or monitoring responsibilities aimed at ensuring compliance by financial institutions and DNFBPs with AML/CFT requirements.

CORRUPTION: According to section (2) of the Anti-Corruption Act No.3 of 2012, ‘corrupt’ means the soliciting, accepting, obtaining, giving, promising or offering of a gratification by way of a bribe or other personal temptation or inducement or the misuse or abuse of public office for advantage or benefit for oneself or another person, and “corruption” shall be construed accordingly.

CROSS BORDER CURRENCY DECLARATION REPORTS: Reports declared to Zambia Revenue Authority by an individual entering or leaving Zambia with an amount in cash, negotiable bearer instruments or both, exceeding USD 5,000 or kwacha equivalent, whether denominated in kwacha or any foreign currency. These reports are transmitted to the FIC by Zambia Revenue Authority.

CURRENCY TRANSACTION REPORT: Reports filed to FIC by reporting entities in relation to any currency transaction in an amount equal to or above USD 10,000 or kwacha equivalent whether conducted as a single transaction or several transactions that appear to be linked.

CURRENCY: The coin and paper money of the Republic, or of a foreign country, designated as legal tender or is customarily used and accepted as a medium of exchange.

DIRECT BIDDING: This is a procurement method where a bid is obtained directly from a single bidder, without competition.

ESAAMLG: One of the Financial Action Task Force styled regional bodies.

FATF: FATF is an inter-governmental body which sets standards and develops and promotes policies to combat money laundering and terrorist financing.

FINANCING OF TERRORISM: Section 2 of the National Anti-Terrorism and Proliferation Act No.6 of 2018 act defines Financing of Terrorism as an act by any person who, irrespective of whether a terrorist act occurs, by any means, directly or indirectly, willfully provides or collects funds or attempts to do so with the intention that the funds should be used or knowing that the funds are to be used in full or in part – (i) to carry out a terrorist act; (ii) by a terrorist; (iii) by a terrorist organization; or (iv) for the travel of a person to a State other than the person’s State of residence or nationality for the purpose of perpetration, planning or preparation of, or participation in, terrorist act or the providing or receiving of terrorist training.

GATEKEEPERS: These are professionals (DNFBPs) that provide non-financial services and include lawyers, accountants.

MONEY LAUNDERING: According to section 2 of the Prohibition and Prevention of Money Laundering Act No.14 of 2001 (as amended), Money Laundering means where a reasonable inference may be drawn, having regard to the objective factual circumstances, any activity by a person -

- a. who knows or has reason to believe that the property is the proceeds of a crime; or
- b. without reasonable excuse, fails to take reasonable steps to ascertain whether or not the property is proceeds of a crime; where the person:
 - i. engages, directly or indirectly, in a transaction that involves proceeds of a crime;
 - ii. acquires, receives, possesses, disguises, transfers, converts, exchanges, carries, disposes, uses, removes from or brings into Zambia proceeds of a crime; or
 - iii. conceals, disguises or impedes the establishment of the true nature, origin, location, movement, disposition, title of, rights with respect to, or ownership of, proceeds of crime”

MUTUAL EVALUATION: An assessment of a country’s measures undertaken to combat money laundering and the financing of terrorism and proliferation of weapons of mass destruction. This includes an assessment of a country’s actions to address the risks emanating from designated terrorists or terrorist organisations.

MVTS: Money or value transfer services (MVTS) refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means

of a communication, message, transfer, or through a clearing network to which the MVTs provider belongs.

Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods. Sometimes these services have ties to particular geographic regions and are described using a variety of specific terms, including hawala, hundi, and fei-chen.

PIP: Prominent Influential Person entails an individual who is or has, been entrusted with a prominent public function by a State or an international or local body or organisations but is not of middle or junior ranking and includes: (i) a head of State or of Government; (ii) a minister; (iii) a member of an executive organ of a political party; (iv) a magistrate, judge and other senior officials of quasi-judicial bodies; (v) a senior military official; (vi) a senior government official; and, (vii) a member of the board or an official in senior management of an administrative or supervisory body, or a state-owned enterprise or statutory body.

PREDICATE OFFENCES: According to FATF, predicate offences are specified “unlawful activities” whose proceeds, if involved in the subject transaction, can give rise to prosecution for money laundering.

PROLIFERATION FINANCING: Section 2 of the National Anti-Terrorism and Proliferation Act No.6 of 2018 act defines Proliferation Financing as an act by any person who by any means, directly or indirectly, willfully or negligently provides funds or financial services to be used or knowing that they are to be used in whole or in part for proliferation, the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling, supply, sale or use of nuclear, ballistic, chemical, radiological or biological weapons or any other weapon capable of causing mass destruction and their means of delivery and related materials including both technologies and dual-use goods used for non-legitimate purposes, including technology, goods, software, services or expertise, in contravention of this Act or, where applicable, international obligations derived from relevant Security Council Resolutions;

SUSPICIOUS TRANSACTION REPORT: This a report submitted on suspected or attempted money laundering, financing of terrorism or proliferation or any other serious offence whether in form of a data message or otherwise.

TECHNICAL COMPLIANCE: Assesses an entity’s compliance with laws, regulations and any other legal instruments it has in place to combat money laundering

and the financing of terrorism and proliferation.

WIRE TRANSFER: Entails any transaction carried out on behalf of an originator through a financial institution or payment system including an institution that originates the wire transfer and an intermediary institution that participates in completion of the transfer by electronic means with a view to making an amount of money available to a beneficiary.

NOTES



NOTES



NOTES





FINANCIAL INTELLIGENCE CENTRE

P.O Box 30481, Lusaka, Zambia

Telephone: +260 211 220 254 +260 211 238 230

www.fic.gov.zm