MONEY LAUNDERING AND TERRORIST FINANCING

TRENDS
REPORT
2018

“Countering Money Laundering, Terrorist Financing and Other Financial Crimes”
THE FINANCIAL INTELLIGENCE CENTRE

THE 5TH MONEY LAUNDERING AND TERRORIST FINANCING TRENDS REPORT, 2018
# Table of Contents

ACRONYMS....................................................................................................................6  
MESSAGE FROM THE DIRECTOR GENERAL.................................................................7  
1.0 PURPOSE...................................................................................................................9  
2.0 BACKGROUND OF THE FIC .................................................................................9  
3.0 ACHIEVEMENTS ....................................................................................................9  
4.0 DISSEMINATIONS .................................................................................................10  
5.0 TRENDS..................................................................................................................11  
5.1 STR TRENDS BY PREDICATE OFFENCE ...............................................................11  
5.1.1 Corruption .........................................................................................................11  
5.1.2 Tax Evasion .......................................................................................................13  
5.1.3 Cyber Fraud .......................................................................................................14  
5.1.4 Environmental crimes .......................................................................................14  
5.2 STR TRENDS IN DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS (DNFBPS) SECTOR ........................................................................14  
5.3 OTHER TRENDS OBSERVED ..............................................................................15  
5.3.1 Private Companies funding political party activities ......................................15  
5.3.2 Irregular Immigration Status ...........................................................................15  
6.0 TRENDS IN CURRENCY TRANSACTION REPORTS ............................................16  
6.1 DNFBP’S USE OF CASH ......................................................................................16  
6.2 UNUSUAL FINANCIAL TRANSACTIONS .............................................................16  
6.3 UNDERVALUATION OF PRECIOUS STONES .................................................16  
7.0 EMERGING RISKS ...............................................................................................17  
8.0 CASE STUDIES .....................................................................................................17  
9.0 STATISTICS ...........................................................................................................23  
9.1 SUSPICIOUS TRANSACTION REPORTS AND SPONTANEOUS DISCLOSURE REPORTS ...............................................................23  
9.2 SPONTANEOUS DISCLOSURE REPORTS .........................................................25  
9.3 CURRENCY TRANSACTION REPORTS ..............................................................25  
10.0 CROSS BORDER DECLARATION REPORTS .......................................................26
<table>
<thead>
<tr>
<th>ACRONYMS</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AML/CFT</td>
<td>Anti-Money Laundering/Countering the Financing of Terrorism</td>
</tr>
<tr>
<td>AMLA</td>
<td>Anti- Money Laundering Authority</td>
</tr>
<tr>
<td>AML</td>
<td>Anti-Money Laundering</td>
</tr>
<tr>
<td>BO</td>
<td>Beneficial Ownership</td>
</tr>
<tr>
<td>CBDR</td>
<td>Cross Border Declaration Report</td>
</tr>
<tr>
<td>CTR</td>
<td>Currency Transaction Report</td>
</tr>
<tr>
<td>DNFBP</td>
<td>Designated Non-Financial Businesses and Professions</td>
</tr>
<tr>
<td>ESAAMLG</td>
<td>Eastern and Southern Africa Anti Money Laundering Group</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force</td>
</tr>
<tr>
<td>FIC</td>
<td>Financial Intelligence Centre</td>
</tr>
<tr>
<td>FIC Act</td>
<td>Financial Intelligence Centre Act</td>
</tr>
<tr>
<td>IFFs</td>
<td>Illicit Financial Flows</td>
</tr>
<tr>
<td>LAZ</td>
<td>Law Association of Zambia</td>
</tr>
<tr>
<td>LEA</td>
<td>Law Enforcement Agency</td>
</tr>
<tr>
<td>ML</td>
<td>Money Laundering</td>
</tr>
<tr>
<td>ME</td>
<td>Mutual Evaluation</td>
</tr>
<tr>
<td>ML/TF</td>
<td>Money Laundering/Terrorist Financing</td>
</tr>
<tr>
<td>MVTS</td>
<td>Money Value Transfer Services</td>
</tr>
<tr>
<td>NGO</td>
<td>Non – Governmental Organization</td>
</tr>
<tr>
<td>NRA</td>
<td>National Risk Assessment</td>
</tr>
<tr>
<td>PACRA</td>
<td>Patents and Companies Registration Agency</td>
</tr>
<tr>
<td>PEPs</td>
<td>Politically Exposed Persons</td>
</tr>
<tr>
<td>PF</td>
<td>Proliferation Financing</td>
</tr>
<tr>
<td>SDR</td>
<td>Spontaneous Disclosure Report</td>
</tr>
<tr>
<td>STR</td>
<td>Suspicious Transaction Report</td>
</tr>
<tr>
<td>TF</td>
<td>Terrorist Financing</td>
</tr>
<tr>
<td>ZICA</td>
<td>Zambia Institute of Chartered Accountants</td>
</tr>
<tr>
<td>ZIEA</td>
<td>Zambia Institute of Estate Agents</td>
</tr>
</tbody>
</table>
MESSAGE FROM THE DIRECTOR GENERAL

2018 was a remarkable year for the Financial Intelligence Centre (FIC) marked by its admission into the Egmont Group of Financial Intelligence Units. Being a member of the Egmont Group is expected to further improve the effectiveness of the FIC in the execution of its mandate, especially the ability to exchange information with over one hundred and sixty (160) jurisdictions.

The FIC continued to implement a robust strategic agenda focused on contributing to the prevention and detection of money laundering and the countering of the financing of terrorism. In this regard, the FIC extended its outreach to the public through education and general awareness of ML and TF.

During the year, the FIC disseminated 80 reports of suspected ML and TF to Law Enforcement Agencies involving suspected financial crimes valued at ZMW 6.1 billion or about USD 520 million.

Zambia was subject of a Mutual Evaluation in 2018 by the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG). The purpose of the Mutual Evaluation, which was coordinated by the FIC, was to determine the extent to which Zambia is compliant with the Financial Action Task Force (FATF) standards and the effectiveness of the AML/CFT regime in Zambia. The report setting out the results of the Mutual Evaluation is due for publication in 2019.

In this regard, the FIC wishes to thank the Government of the Republic of Zambia for the material and moral support given to this important national assignment. The FIC further extends its gratitude to Government agencies, private institutions and other stakeholders that participated in the assessment process.

The 2018 Trends Report on AML/CFT is intended to increase public awareness and understanding of Zambia’s AML/CFT regime. It provides a synopsis of suspicious financial transactions analysed and related financial crimes identified by the FIC during the year. Such information is critical in supporting Zambia’s response towards the prevention and detection of ML/TF and PF.

Zambia operationalized a currency transaction reporting threshold in January 2017 following the issuance of the Financial Intelligence Centre (Prescribed Thresholds) Regulations through Statutory Instrument (S.I) No. 52 of 2016.

The S. I. requires reporting entities to report all currency transactions to the Financial Intelligence Centre equal to or above USD 10,000 or its equivalent. This is an automated system and therefore does not imply any illegality in what is reported but helps in strategic analysis. The requirement for reporting is part of the measures recommended by the FATF. The measures are intended to improve the ability of countries to prevent and detect illicit sources and uses of cash. This helps in the combating of the twin evils of money laundering and terrorist financing. It further makes up part of the international tool kit against illicit financial flows.

The Eastern and Southern Africa Anti Money Laundering Group (ESAAMLG) has just concluded a mutual evaluation of the AML/CFT systems in Zambia and the country was compliant with the requirement of setting currency thresholds as per the FATF standards. Further, it should be noted that the currency thresholds set by the S.I are not equivalent to limits. Customers are therefore not prohibited from transacting in any currency amount above US$10,000. Most of the countries in the region have set currency transaction thresholds below US$10,000.
During 2018, the system operated optimally.

The fact that almost all countries in the global community are members of FATF or FATF styled regional bodies suggests that if these thresholds had a negative impact on economic performance, the world would be in perpetual recession. For purposes of economic policy, the country needs to encourage more usage of electronic payment systems in order to increase financial transparency.

Given the socio-economic developmental challenges that Zambia faces, it is crucial that national resources are safe-guarded and applied in accordance with the Government’s plans and priorities. For example, Money Laundering reduces revenue for the government as laundered funds are untaxed. Reduced revenues also limit the Governments’ ability to provide public goods and services such as education, health and other social amenities. Such illicit funds also have the potential to destabilize Zambia’s financial payment systems and encourage corrupt practices.

All public and private institutions including the general public are therefore encouraged to actively participate in Zambia’s quest to become a “financial crimes free” nation.

Mary Chirwa (Ms.)
Director General
Financial Intelligence Centre
1.0 PURPOSE

The publication of the 2018 Money Laundering/Terrorist Financing (ML/TF) Trends report is issued pursuant to section 5(2)(e) of the FIC Act, No. 4 of 2016 which mandates the FIC to inform the public on the ML/TF trends. Further, the Trends report is published in line with the international AML/CFT standards which require jurisdictions to publish ML/TF typologies and trends. The report may influence policy formulation and assist stakeholders in the AML/CFT regime through strengthening of cooperation and better understanding of risks, trends and methods being applied by suspected criminals in the AML/CFT environment.

2.0 BACKGROUND OF THE FIC

The FIC was established in 2010 following the enactment of the Financial Intelligence Centre Act, No. 46 of 2010 as amended by the Act No. 4 of 2016 (the Act). It became operational in November, 2013. Section 5 of the Act provides that the FIC shall be the sole designated agency responsible for the receipt, requesting, analysing and disseminating of the disclosure of suspicious transaction reports to competent authorities for investigations and prosecution. Further, the FIC receives Currency Transaction Reports (CTRs) and the Cross Border Currency Declaration Reports (CBCDRs).

The FIC undertakes tactical and strategic analysis. Tactical analysis aims to detect suspected ML/TF through identification of sources of proceeds of crime, links between criminal associates and syndicates and the dissemination of intelligence reports to LEAs and other competent LEAs. Information gathered during the year is collated to identify trends, risks and methods used in ML/TF which is published in the trends report. This is in fulfilling the FIC’s mandate of educating the public on ML/TF.
3.0 ACHIEVEMENTS

The FIC was admitted into the Egmont Group of Financial Intelligence Units (FIUs) on 26th September 2018. This development creates greater opportunity for sharing financial intelligence with foreign jurisdictions.

The report is expected to be published on the ESAAMLG website in June, 2019 following the approval by the Council of Ministers.

In 2018, the FIC disseminated 80 financial intelligence reports related to suspected offences of money laundering and terrorist financing to LEAs.

During 2018, the FIC coordinated the Mutual Evaluation of Zambia’s AML/CFT regime under the auspices of the AML/CFT National Task Force of Senior Officials. The ME process involved the participation of both the public and private sector stakeholders. This assessment was for the country’s technical compliance to the FAFT standards and the extent to which the regime was effective in preventing money laundering and terrorist financing.

The FIC during 2018 led two important regional projects. One was a typology study on procurement corruption and associated money laundering in the ESAAMLG region. The other was the development of guidance on effective methods on gathering financial intelligence. Both reports are due for release in 2019.
4.0 DISSEMINATIONS

In 2018, the Centre analysed 176 suspicious transaction reports, of which 80 were disseminated to Law Enforcement Agencies on suspicions covering: tax evasion, fraud, corruption and money laundering. The total value of the suspected offences in the disseminated cases was estimated at ZMW 6.1 billion (or about USD 520 million) which includes tax assessments by ZRA amounting to ZMW 62 million. The assessment period was from 1st January 2018 to 30th September 2018. The breakdown of offences covered in the disseminated reports is shown below:

<table>
<thead>
<tr>
<th>No.</th>
<th>Suspected Offence</th>
<th>Estimated loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Tax Evasion</td>
<td>ZMW1 Billion</td>
</tr>
<tr>
<td>2.</td>
<td>Corruption</td>
<td>ZMW 4.9 Billion</td>
</tr>
<tr>
<td>3.</td>
<td>Theft</td>
<td>ZMW 110 Million</td>
</tr>
<tr>
<td>4.</td>
<td>Fraud</td>
<td>ZMW 54 Million</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>6.1 Billion</td>
</tr>
</tbody>
</table>

1.1 Possible violations on which the reports were disseminated covered the following:

- Possible violations under the Income Tax Act chapter 323 and Customs and Excise Act chapter 322.
- Possible violations under the Penal Code chapter 87.
- Possible violations under the Forfeiture of Proceeds of Crime Act No. 19 of 2010.
- Possible violations of the Prohibition and Prevention of Money Laundering Act No. 44 of 2010 (as amended)
- Possible violations of the Anti-Corruption Commission Act No. 3 of 2012

5.0 TRENDS

The trends observed in 2018 were in many ways similar to those of preceding years. For example, in 2017, the Centre disseminated reports involving suspicious financial transactions valued at ZMW 4.5 billion, increasing to ZMW 6.1 billion in 2018. This was mainly attributed to the increase in the value of transactions related to corruption in the disseminations.

5.1 STR Trends by Predicate Offence

5.1.1 Corruption

The most prevalent forms of corruption noted in 2018 were those involving bribery, self-dealing/conflict of interest. During the year, the Centre disseminated reports on corruption with an estimated value of ZMW 4.9 Billion.

Public Procurement Activities

Public procurement activities were significantly vulnerable to corruption. Government purchasing procedures generally involve:

- Drawing up of specifications
- Tender process
- Awarding stage
- Implementation of the contract

Certain specifications are manipulated to disadvantage other bidders. After the specifications have been drawn, the tender process commences. This involves the bidding and the awarding of contracts. The implementation stage is also susceptible to corruption as most contracts are not performed as per contractual obligation. Procurement corruption has led to the crowding out of legitimate businesses. It has also increased the cost of public projects. The specific methods by which the funds were laundered were;

i) Use of shell Corporate Vehicles and Trusts

Shell Corporate Vehicles are registered companies that are non-operational and do not have known physical addresses. From cases analysed in 2018, shell companies were used to obtain contracts from Government institutions and launder proceeds of crime. It was also noted that some shell companies were used to conceal the identity of beneficial owners. Other cases analysed indicated that some contracts were awarded prior to formation of the corporate vehicle.

ii) Use of Gatekeepers

The FIC noted the high usage of gatekeepers such as law firms and accounting/audit firms to facilitate corrupt activities. The specific activities included using accounts of law firms to layer transactions, purchase property and to distribute cash to beneficial owners. In some instances, the perpetrators were holders of public office, and part of their responsibility was to regulate members for AML/CFT purposes.

iii) Use of Domestic Financial Institutions

These included banks, micro-finance institutions, pension funds and insurance companies. A number of cases that were analyzed involved placement of proceeds of crime and transfer to jurisdictions outside Zambia.

iv) Use of Nominees

The FIC noted a continuing trend of the use of associates or nominees or family members to hide beneficial ownership of corporate vehicles and to own property.

v) Ineffective controls in public institutions

In some instances, the FIC observed a trend where “Companies” not registered with the Patents and Companies Registration Agency (PACRA) were awarded public contracts. Most of these companies were connected to Politically Exposed Persons (PEPs).

vi) Dispossession of property

The FIC observed dispossession of property through force and intimidation of legal owners and Law Enforcement officers. Perpetrators included Zambians and foreign nationals.
**Recommendations**

**Use of shell corporate vehicles**

The Public Procurement Act should be reviewed to prohibit participation of shell corporate vehicles in public procurement. This should include partnerships where the sole purpose is for the shell company to obtain the contract which is executed by some other company.

Further, the rules should focus on the persons behind the incorporated entity rather than the entity to avoid repeat offenders defrauding Government through use of new Corporate Vehicles.

**Use of Gate Keepers**

Professional bodies such as ZICA and LAZ should effectively supervise institutions under their scope of influence to ensure criminal elements do not hijack the operations of the supervisory bodies.

**Use of Domestic Financial Institutions**

The FIC has observed willful blindness in the case of some reporting institutions in filing of STRs. The sanctions regime has emphasis on criminal sanctions for non-reporting. This may not always be appropriate for the nature of relationship between an FIU and the reporting entity.

It is therefore recommended that the Act is amended to allow for more flexible administrative sanctions, including financial penalties.

**Beneficial ownership**

The new Companies Act that requires disclosure of beneficial ownership in the public company registry came into force in 2018. It is recommended that the requirement be extended to other forms of business entities such as trusts and cooperatives to ensure transparency across the regime.

**5.1.2 Tax Evasion**

In 2018, the Centre analysed reports related to tax evasion. Tax evasion schemes involve an individual or corporation misrepresenting their income to the Zambia Revenue Authority (ZRA). Many of the cases analysed on suspected tax evasion involved Small and Medium Enterprises (SMEs). Most of these entities were either not registered for tax purposes or were not tax compliant.

Some of the cases analysed were based on the following:

False accounting: Some companies overstated their expenditure and this reduced their profits and hence their tax obligations.

Group company loans: some companies externalized funds to their parent companies. The same companies would then receive the funds in the form of loans. This reduced their tax liability as interest on the loans received tax relief.

Use of personal accounts for business: it was observed that individuals were using personal accounts for business purposes. This affected the completeness and accuracy of business records hence compromising their tax compliance.
**Recommendation**

It is recommended that presumptive tax is extended to other sectors, especially small enterprises such as: barber shops, saloons and micro retail stores. This will reduce the administrative burden of tax collection of taxes whilst also increasing on both the tax payer compliance.

### 5.1.3 Cyber Fraud

During the year 2018, the Centre disseminated two (2) cases valued at ZMW 2 million involving cyber-crime.

The cases involved hackers infiltrating the networks of various organizations without being detected and impersonating their suppliers, customers and even employees only to defraud third parties into losing money.

In addition, a number of unsuspecting members of the public were lured into disclosing their personal bank and identification details via phone or e-mail only to be defrauded. With the rise of mobile money transactions, the Centre has seen an increase in citizens being defrauded through Short Messages Services (SMS) platforms.

Other reports received by the Centre in 2018 were related to social media fraud where individuals were deceived into making purchases from fraudulent vendors who advertised on social media.

**Recommendations**

- Service providers need to invest more in customer awareness of the hazards/risks associated with cyber based platforms.
- Stronger controls by reporting entities and their agents to prevent fraudsters from hacking their systems.
- Service providers to develop mechanisms for the identification of beneficiaries of money value transfers.

### 5.1.4 Environmental crimes

The Centre continues to see timber sales in regions where endangered Rosewood “Mukula” is indigenous. The Centre has analysed cases in which individuals trading in the prohibited Mukula declared timber as their source of funds.

In 2018, the Centre received Suspicious Transaction Reports (STRs) related to timber valued at ZMW 2,156,000. Many of the individuals in the illegal trade of Mukula established other businesses through which these proceeds were laundered. The areas most affected were Manyinga and Mufumbwe in North Western Province. The Centre further noted that foreign nationals continued to engage locals to illegally harvest the endangered tree for subsequent transportation out of the country, mostly to Asia.

### 5.2 STR Trends in Designated Non-Financial Businesses and Professions (DNFBPs) Sector

During the year 2018, DNFBPs continued to be used as vehicles for money laundering by criminals. These included law firms, real estate agencies, casinos and motor vehicle dealers.
Law Firms

It was observed that identified law firms assisted suspected criminals to mask the source of funds and aided its reinvestment or movement to foreign jurisdictions. Most cases involved illegally obtained funds transferred to law firms who then facilitated the acquisition of property such as land and motor vehicles on behalf of the launderers. In 2018, the Centre analysed cases related to nine (9) law firms amounting to ZMW 365 Million.

Real Estate

The acquisition of property using laundered funds continued to occur during the year 2018. The Centre observed a discrepancy between the mortgage market and the rising number of housing and office infrastructure. This rise can partly be attributed to an increase in the number of Property Developers. Currently, there is no regulator that oversees the activities of property developers for AML/CFT purposes. Construction provides an easy and undetectable avenue for criminals to launder funds. The placement and layering of the illegal proceeds occur during the construction of property. The Integration of the proceeds of crime occurs when either the property is sold or leased for rental income.

Casinos

Reports analysed by the Centre in 2018 indicated that some casinos do not hold bank accounts in Zambia. It was however noted that persons, especially from foreign jurisdictions working for these casinos, had bank accounts in Zambia that received large cash deposits which were followed by large outward transfers, mostly to their home jurisdictions. Further, some casinos were using employees and shareholders as cash couriers.

The Centre also noted that some of these casinos are not compliant with the local law requirements prescribed by the Zambia Revenue Authority or the Licensing Committee under the Ministry of Tourism and Arts.

5.3 Other Trends Observed

5.3.1 Private Companies funding political party activities

It was noted that some private companies that were awarded public contracts were funding some named political parties. The funds would move from these private companies to prominent individuals linked to the political parties. The cases analysed amounted to ZMW 10 million.

Recommendation

It is recommended that the Registrar of Societies makes it a requirement for all political parties to disclose their sources of funding and submit audited annual financial statements which should also be available for public scrutiny through the appropriate Parliamentary Committee.

5.3.2 Irregular Immigration Status

It has been observed from the reports analysed by the Centre that some Foreign Nationals have continued engaging in business activities without valid permits. These individuals operate unregistered businesses from their places of residence.
Recommendation

It is recommended that financial institutions ensure that all foreign nationals have valid permits during their CDD procedure before account opening.

6.0 TRENDS IN CURRENCY TRANSACTION REPORTS

In 2018, the Centre observed a general increase in the number of CTRs received for individuals while corporate CTRs decreased. During the period under review, the individual CTRs increased by 8,968 from 10,966 received in 2017. This represents an 82% increment from the prior year. On the other hand, the corporate CTRs reduced by 7,008 from 62,303 received in 2017. This represented an 11% decrease from the prior year.

6.1 DNFBP’s use of cash

Designated Non-Financial Businesses and Professions such as lawyers, accountants and real estate agents provide services and products that are susceptible to abuse by criminals to hide the proceeds of crime.

In 2018, the Centre received 145 transactions above the prescribed threshold of USD10,000 or its Kwacha equivalent deposited by these professionals into their corporate accounts. The value of these transactions was ZMW 28,465,441.46 and USD 15,214,189.50. These transactions raise suspicion on the source of the income as legitimately earned funds would be transmitted through appropriate methods such as wire transfers.

6.2 Unusual financial transactions

a) Construction transactions by Corporates

The Centre noted some unusual transactions in the Construction sector where payments for construction services were expected to be made through methods such as cheques, wire transfers as opposed to cash. In 2018, the Centre identified transactions valued at ZMW 86,644,645.85 and USD 8,089,289.44 from deposits made by construction companies. This represents a general increase from 2017 where deposits made by construction companies amounted to ZMW 14,150,918.70 and USD 9,668,421.14.

The use of cash in this sector raises suspicions that the funds could be proceeds of crime.

b) Agricultural transactions by Individuals

During the year 2018, there were a large number of cash transactions above USD10,000 (Kwacha equivalent) relating to agricultural products. These transactions amounted to ZMW 134,062,004 and USD 5,452,852. Maize related transactions were the most prevalent and amounted to ZMW 110,064,958 and USD 5,452,852. The transactions were conducted by Zambian nationals and occurred mostly between March and October 2018.

The USD denominated transactions mostly took place in Chililabombwe town in the Copperbelt province of Zambia. This is a border town and the transactions indicate that the maize was being exported to the Democratic Republic of Congo (DRC). The Kwacha denominated transactions mostly occurred in Lusaka, Choma, Chililabombwe, Petauke, Chipata and Mbala towns respectively.
6.3 Undervaluation of precious stones
The Centre analysed cases relating to trade in precious stones. It was observed that some exporters significantly under-declared the value of the stones. As a result, they reported losses thereby incurring lower tax liabilities.

**Recommendation**

It is recommended that the auctioning of precious stones be done locally.

7.0 EMERGING RISKS

Over the last decade the world has seen an increase in the use of crypto-currencies as a method for transmitting and storing value and as a medium of exchange.

In Zambia, crypto-currency is currently unregulated. This therefore provides a conducive environment for fraudulent activities.

The 2014 FATF report on virtual currencies defines Crypto-currencies as ‘Distributed, open-source math-based peer-to-peer virtual currencies that have no central administrating authority and no central monitoring or oversight’. Some examples of crypto-currencies are Bitcoin, Litecoin and Ripple.

The anonymity characteristic of crypto-currencies have made them a tool for criminals, terrorist financiers and other sanction evaders to move and store illicit funds making them undetectable by law enforcement agencies. Furthermore, the decentralization of crypto-currencies makes it difficult for them to be regulated. The 2018 G20 summit in Argentina resolved that crypto-assets will be regulated using the FATF guidance.

In line with the FATF guidelines, the Centre recommends the following regulations on crypto-currencies;

- Policy formulation to target crypto-currency converters, these are individuals/institutions that provide gateways to the regulated financial system.
- Regulating financial institutions or DNFBPs that send, receive, and store crypto-currencies.

8.0 CASE STUDIES

Case 1: Corruption, Abuse of Office and Money Laundering

PEP N, was alleged to have amassed wealth that was not in line with his expected income within a short period of time. The PEP was alleged to have amassed wealth through suspected corrupt practices with the aid of two other PEPs, his associates (PEP D) and (PEP C).

PEP N influenced the awarding of contracts to foreign construction companies and in return, these companies constructed 49 residential properties for him valued at ZMW 70 million. They further purchased two luxury vehicles for him valued at ZMW 4 million.

With respect to PEP C and PEP D, it was noted that they had acquired four (4) properties valued at ZMW 61,000,000.

A review of the bank accounts of PEP N and PEP C for the period 1st October 2015 to 30th April 2018 revealed the following credit turnover;
PEP N: ZMW 12,000,000
PEP C: ZMW 35,000,000
The case was disseminated for suspected corruption and money laundering to competent authorities.
Case 2: Corruption and Money Laundering

Mr. S, a foreign national resident in Zambia received USD 3 million on his personal account from a European company AS. Upon receipt of the funds, Mr. S withdrew ZMW 5 million in cash and then transferred USD 400,000 to his country of origin. He further transferred USD600,000.00 to a local company CH, where he is a shareholder. Company CH is a Zambian company that was awarded a contract to provide public services. The shareholders are company B based in Zambia, company AS based in Europe and Mr. S, a foreign national resident in Zambia. Company CH was awarded a contract despite being in operation for only three (3) months. This is contrary to Public Procurement Act number 12 of 2008.

Mr. S’s personal accounts further showed substantial inward transfers between 2016 and 2018 from company CH which were followed by transfers totaling USD 3.5 million to various individuals, including public officials. Mr. S further received USD 5 million from company CH.

CH’s bank account revealed that there are two signatories, Mr. S and Mr. M, a partner at an audit firm. It was observed that there were monthly transfers from CH account to the account of the audit firm with the reference stating that the funds were meant for salaries.

The movement of funds among the procuring entity, Company CH and Company AS raised a red flag.

The funds transferred to public officials in strategic institutions by Mr. S had no economic rationale. The funds were used to purchase property by the public officials. Further, huge cash withdrawals were made by Mr. S for suspected third party beneficiaries.

The matter was disseminated to competent authorities for suspected money laundering and corruption.
Case 3: Suspected Terrorist Financing

Two foreign nationals X and Y incorporated company D in Zambia. Company D held bank accounts with bank B. Mr. X requested the bank to amend his name, date of birth and nationality. Upon receipt of this request, the bank performed customer due diligence and adverse information on the new credentials was revealed. The new name was linked to a terrorist group in Country Q within Africa. Mr. X made multiple forex purchases using his company account to fund his travel from Zambia to the African Country where terrorist activities are rampant. The forex purchases by Mr. X were suspected to be funding terrorist activities in Country Q.

The matter was disseminated to competent authorities for further investigation.

Case 4: Bribery & Corruption, Tax Evasion & Money Laundering

Company ZD and its proprietor PQ, a PEP, allegedly received funds from foreign construction companies who were awarded contracts by the public institution. The funds were remitted to company ZD which operates as a financial institution without any economic rationale. The shareholder also received cash deposits in his personal account (Account 2) amounting to ZMW 1.4 million.

The funds received amounted to ZMW 6.5 million. PEP PQ subsequently transferred the funds to third parties of a Non-Profit Organisation (NPO). Of the funds deposited, an amount of ZMW 750,000 was transferred to the account of PEP J who purchased property. A further ZMW 5 million was withdrawn in the form of cash by shareholders.
9.0 STATISTICS

9.1 Suspicious Transaction Reports and Spontaneous Disclosure Reports

Table (i) Number of STRs received

The table below shows the number of STRs received by year

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>487</td>
</tr>
<tr>
<td>2015</td>
<td>767</td>
</tr>
<tr>
<td>2016</td>
<td>719</td>
</tr>
<tr>
<td>2017</td>
<td>1664</td>
</tr>
<tr>
<td>2018</td>
<td>799</td>
</tr>
</tbody>
</table>

Table (ii) Chart on number of reports for the last 5 years

In 2018, a total of 799 reports were received from various Reporting Entities. Of these, 724 were Suspicious Transaction Reports (STRs) and 75 were Spontaneous Disclosure Reports (SDRs).

The Banks accounted for 89.5% of STRs received. These reports were primarily triggered by unusual cash transactions. The high number of reports from this sector is a result of a successful campaign by the FIC and the banking sector being in a well regulated industry.

Further, the banking sector is, by far, the largest in terms of customer base and asset value in the financial sector.
### Table (iii) Chart on STRs received per sector

<table>
<thead>
<tr>
<th>Sector</th>
<th>Number Received</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banks</td>
<td>648</td>
<td>89.5%</td>
</tr>
<tr>
<td>MVTs</td>
<td>58</td>
<td>8.0%</td>
</tr>
<tr>
<td>Insurance</td>
<td>2</td>
<td>0.3%</td>
</tr>
<tr>
<td>Casinos</td>
<td>1</td>
<td>0.1%</td>
</tr>
<tr>
<td>Microfinance</td>
<td>12</td>
<td>1.7%</td>
</tr>
<tr>
<td>Bureaus</td>
<td>1</td>
<td>0.1%</td>
</tr>
<tr>
<td>Real Estate</td>
<td>1</td>
<td>0.1%</td>
</tr>
<tr>
<td>Building Society</td>
<td>1</td>
<td>0.1%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>724</strong></td>
<td><strong>100.0%</strong></td>
</tr>
</tbody>
</table>

In 2018, the Centre received Suspicious Transaction Reports (STRs) bordering on various suspicions as per the table below. The STRs received by the Centre are reported on the basis of the suspicion surrounding the transaction and not the value of the transaction.

### Table iv) Nature of suspicions reported

<table>
<thead>
<tr>
<th>Reason for Suspicion</th>
<th>Cases reported</th>
<th>Amount</th>
<th>Percentage of cases reported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity inconsistent with customer profile</td>
<td>162</td>
<td>143,012,609.97</td>
<td>22.4%</td>
</tr>
<tr>
<td>Avoiding reporting obligations</td>
<td>14</td>
<td>259,076,981.00</td>
<td>1.9%</td>
</tr>
<tr>
<td>Fraud/ATM Fraud/Credit Card fraud</td>
<td>31</td>
<td>6,818,823.37</td>
<td>4.3%</td>
</tr>
<tr>
<td>Internet Fraud/Phishing</td>
<td>11</td>
<td>356,583.50</td>
<td>1.5%</td>
</tr>
<tr>
<td>Irregular or unusual International banking activity</td>
<td>15</td>
<td>14,280,988.61</td>
<td>2.1%</td>
</tr>
<tr>
<td>Large or unusual cash deposit</td>
<td>186</td>
<td>103,267,454.39</td>
<td>25.7%</td>
</tr>
<tr>
<td>Large or unusual cash withdrawals</td>
<td>9</td>
<td>2,386,623.00</td>
<td>1.2%</td>
</tr>
<tr>
<td>Large or unusual inward remittance</td>
<td>48</td>
<td>165,424,192.44</td>
<td>6.6%</td>
</tr>
<tr>
<td>Large or unusual outward remittance</td>
<td>27</td>
<td>130,635,073.14</td>
<td>3.7%</td>
</tr>
<tr>
<td>Many third parties making deposits</td>
<td>11</td>
<td>3,357,828.00</td>
<td>1.5%</td>
</tr>
<tr>
<td>Person – Suspicious Behaviour</td>
<td>146</td>
<td>85,110,077.81</td>
<td>20.2%</td>
</tr>
<tr>
<td>Unusual business practices</td>
<td>26</td>
<td>40,401,335.71</td>
<td>3.6%</td>
</tr>
<tr>
<td>Unusually large foreign currency transaction</td>
<td>11</td>
<td>71,989,218.00</td>
<td>1.5%</td>
</tr>
<tr>
<td>Watch listed individual/organization</td>
<td>10</td>
<td>32,000.00</td>
<td>1.4%</td>
</tr>
<tr>
<td>Other</td>
<td>17</td>
<td>909,225.00</td>
<td>2.3%</td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td><strong>724</strong></td>
<td><strong>1,027,059,013.94</strong></td>
<td><strong>100.0%</strong></td>
</tr>
</tbody>
</table>
The table above shows the number of STRs submitted by type of suspicion and the amount thereof.

The highest number of STRs received were based on “Large or unusual cash deposits”. This occurred mostly when individuals made cash deposits that were significantly above their declared income.

A number of STRs reported were on the basis of “person- suspicious behavior”. This mostly involved customers, who are public officials and ordinary citizens, opening accounts in the name of a family member who begins making large deposits not consistent with the known sources of legitimate income.

Further, other STRs received were based on “Activity inconsistent with customer profile”. Cases analysed indicated that customers declared a lower income at account opening but transacted in amounts that were significantly higher than what was declared. This is an indication that the customer could have other sources of income which are not disclosed to the bank. It could also indicate that the bank does not update their customer records when a customer’s profile has changed.

### 9.2 Spontaneous Disclosure Reports

The Centre received 75 Spontaneous Disclosure Reports (SDR) in 2018 bordering on fraud, corruption, theft and tax evasion.

#### Table (v) Nature of suspicion reported

<table>
<thead>
<tr>
<th>Reason for Suspicion</th>
<th>Cases reported</th>
<th>Values (ZMW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corruption</td>
<td>22</td>
<td>578,281,000</td>
</tr>
<tr>
<td>Fraud/ATM Fraud/Credit Card fraud/Internet fraud/Cheque fraud</td>
<td>11</td>
<td>1,487,752.78</td>
</tr>
<tr>
<td>Tax Evasion</td>
<td>5</td>
<td>Nil</td>
</tr>
<tr>
<td>Theft</td>
<td>5</td>
<td>969,820</td>
</tr>
<tr>
<td>Poaching/Wildlife trafficking</td>
<td>2</td>
<td>70,356,000</td>
</tr>
<tr>
<td>Other</td>
<td>30</td>
<td>Nil</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>75</strong></td>
<td></td>
</tr>
</tbody>
</table>

### 9.3 Currency Transaction Reports

Reporting entities are required by law to submit Currency Transaction Reports (CTRs) to the Financial Intelligence Centre for all transactions equal to or above the Kwacha equivalent of ten thousand United States Dollars (USD 10,000).

In 2018, the Centre received a total of 75,592 CTRs (55,658 corporates and 19,934 individuals) from various reporting entities. The largest numbers of transactions were denominated in Zambian Kwacha, followed by United States dollars and other currencies. The mean value of transactions received per currency is depicted below in table vi.
Table vi : Corporate CTRs by currency (Jan – Dec 2018)

<table>
<thead>
<tr>
<th>Currency</th>
<th>Number of Transactions</th>
<th>Value by Currency</th>
<th>Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZMW</td>
<td>46,780</td>
<td>10,808,403,865.09</td>
<td>231,047.54</td>
</tr>
<tr>
<td>USD</td>
<td>8869</td>
<td>1,869,864,663.88</td>
<td>210,831.51</td>
</tr>
<tr>
<td>CNY</td>
<td>1</td>
<td>65,385.12</td>
<td>65,385.12</td>
</tr>
<tr>
<td>EURO</td>
<td>1</td>
<td>28,750.00</td>
<td>28,750.00</td>
</tr>
<tr>
<td>ZAR</td>
<td>4</td>
<td>2,710,350.00</td>
<td>2,710,350.00</td>
</tr>
<tr>
<td>GBP</td>
<td>3</td>
<td>351,873.68</td>
<td>117,291.23</td>
</tr>
</tbody>
</table>

10.0 CROSS BORDER DECLARATION REPORTS

In the year 2018 the Centre received Cross border declaration reports only from Kasumbalesa border in Chililabombwe. No reports were received from other border towns. A total of 2,169 were received, valued at USD 102,696,488. It was observed that most of the transactions were performed by Congolese Nationals who represented 97% of the total reports received. The remaining 3% involved Zambians and other Nationals. The final destination or use of the funds is not known.