

MONEY LAUNDERING TYPOLOGIES IN MALAWI

September 2011

Table of Contents

Abbreviations 2

Message from the Director’s Office 3

1.0 Introduction..... 4

 Suspicious Transaction Reports 5

2.0 Typologies 7

 2.1 Fraud 7

 2.2 Tax Evasion..... 8

 2.3 Trade-based Money Laundering..... 8

3.0 Money Laundering Case Studies..... 9

 3.1 Money laundering through tax evasion 9

 3.2 Laundering of money stolen from Government 11

 Case 3.3 Defrauding of Government through payment for undelivered goods and services. . 13

 3.4 Fraud and Money laundering through a series of companies 14

 3.5 Use of foreign remittance for capital flight 15

 3.6 NGO Director illegally used charity funds for personal gain. 16

 3.7 Trade based money laundering..... 17

 3.8 Capital flight through agents based abroad..... 18

4.0 Conclusion..... 19

Abbreviations

ACB	Anti-Corruption Bureau
AGD	Accountant General's Department
AUSTRAC	Australian Transactions Reporting and Analysis Centre
FFU	Fiscal and Fraud Unit of Malawi Police Service
FIU	Financial Intelligence Unit
KYC	Know Your Client
LCTR	Large Currency Transaction Report
LEA	Law Enforcement Agency
ML	Money Laundering
MRA	Malawi Revenue Authority
RBM	Reserve Bank of Malawi
STR	Suspicious Transaction Report
TF	Terrorist Financing
VAT	Value Added Tax

Message from the Director's Office

I am pleased to present to the public the first Money Laundering typologies report from the Republic of Malawi compiled by the Financial Intelligence Unit (FIU). Typologies are generally methods or trends through which proceeds of crime are disguised by criminals to appear to be originating from legitimate sources.

There are four major methods by which criminals move money in the country for purposes of disguising their origins and integrate it into the formal economy. The methods are: fraud and corruption, general fraud, tax evasion and trade-based money laundering.

Public officials and some civil servants engage in unscrupulous ways of embezzling funds from the government. This takes the form of offering payment for fictitious transactions or bribing government officers to get certain favours.

The tendency of defrauding institutions has not spared private sector organisations. Some employees of private sector organisations connive with financial institutions to arrange swindling of company funds through preparation of forged cheques and other means.

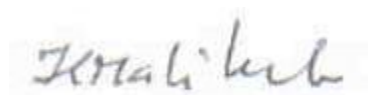
Tax evasion is another grey area which serves as source of money for criminals. The FIU has worked with the Malawi Revenue Authority (MRA) to deal with this crime. There have been a number of cases involving under-invoicing of imports and under-declarations of corporate profits made to evade tax.

Through importing of goods, some criminals have been involved in over-invoicing of imports in order to flight capital from the country.

The compilation of this report is therefore a very significant milestone as the report will help stakeholders in the country to modify their strategies and channel their efforts towards combating the criminal activities as highlighted in this document.

For this work to be possible, there were concerted efforts. The FIU worked with law enforcement agencies and financial institutions in the country. These provided valuable information contained in this report. In particular, the FIU is indebted to the Malawi Revenue Authority, Fiscal and Fraud Unit of the Malawi Police Service and the Department of Immigration.

Thank you for taking interest in reading this document. It is my conviction that you will continue committing yourself to fighting money laundering and terrorist financing. If you have not yet joined this fight, let this serve as a timely invitation to you.



Tom Malikebu

Acting Director, Malawi FIU

1.0 Introduction

The mission of the Financial Intelligence Unit (FIU) is to prevent and detect Money Laundering, Terrorist Financing and other financial crimes by providing quality intelligence to law enforcers and foreign FIUs. Its commitment extends to the provision of training; implementation of an effective compliance framework to reduce ML (money laundering) and (terrorist financing) TF risks; and public awareness on the trends of ML & TF and the impact these have on the economic and financial stability of Malawi.

As one way of advancing its mission, the FIU has developed typologies on ML techniques taking place in the country. The typologies have been developed for the first time and this has been possible courtesy of the Australian Transaction Reports and Analysis Centre (AUSTRAC) who provided training in this area to the FIU in March 2011.

This report has been developed through close cooperation, interaction and sharing of information with law enforcement agencies (LEAs); namely; Fiscal and Fraud Unit of Malawi Police Service (FFU), MRA and Immigration Department. Apart from information from the LEAs, the FIU deployed high level macro-analysis of information in its database which included large currency transaction reports (LCTRs) and suspicious transaction reports (STRs) as well as other publicly available information. The LCTRs and STRs were mainly filed by the banks and the FIU appreciates the sector's role in fighting money laundering in the country.

This report has been prepared in such a way that it informs the financial industry and the wider population at large about methods which criminals are using to conceal and launder proceeds of crimes. Successful commission of the crimes gives the criminals impetus to commit further financial crimes and in so doing damaging the socio-economic fabric of the country. Furthermore, through this report, the LEAs will be empowered to determine whether or not financial crime cases being investigated from time to time have links with money laundering.

In this report, case studies have been used to illustrate the trends being used for money laundering in the country. The cases took place over the past four years and they are only part of many that were handled by law enforcement during the stated period. Some could not be shared in this report because legal processes had not been concluded at the time of publishing this report while others were sensitive in nature.

The report also provides challenges faced by stakeholders in the country during investigation and prosecution of cases involving money laundering.

Suspicious Transaction Reports

Suspicious Transaction Reports (STRs) continue to be the main source of significant analysis conducted by the FIU. Some of the cases used in this report are an outcome of quality STRs from financial institutions. However, reporting on such matters has been erratic with other reporting institutions contributing no report for the past twelve months.

An effective Know Your Customer (KYC) program is instrumental to identifying suspicious activities. However, lack of verification of identity and place of business has plagued most financial institutions in the country. Through its analysis, the FIU has uncovered several cases where some banks have been failing to identify locations of their clients. Surprisingly, the banks continue to maintain relationships with such business entities which transact millions of Kwacha.

Some of the grounds of suspicion in filed STRs were:

- Large currency transactions in inactive accounts;
- Regular transfer of funds without making business sense;
- International funds transfers using fraudulent documents;
- Transactions being inconsistent with customer profile;
- Immediate withdrawal of funds which were barely cleared;
- Multiple transactions within a short time; and
- Smurfing (the act of performing multiple financial transactions below a threshold to avoid the currency reporting requirements)

On suspicious transaction reporting, the FIU continues to provide feedback to banks through sanitized cases. This feedback is based on the database of cases which have been analyzed since 2008.

The FIU endeavors to meet law enforcement agencies on a quarterly basis. It is through these interactions that patterns of criminal activities are unearthed and

strategies to counter them agreed upon. Collaboration with LEAs also helps recovery of revenues that would otherwise be lost through tax evasion and other illegal activities. Penalties are also imposed on such entities to deter others from indulging in such malpractices.

2.0 Typologies

The Vision of the FIU is to be leaders in the fight against Money Laundering, Terrorist Financing and related financial crimes thereby contributing towards the economic and financial stability of Malawi.

Criminals are always looking for opportunities to acquire profit from crime. When a series of money laundering schemes appear to be fashioned in a similar manner or using the same methods, those schemes are generally classified as typologies. By reviewing cases, the FIU was able to identify a number of typologies associated with fraud, tax evasion and capital flight. Transnational trade, booming real estate development and technological advancement have contributed to committing of the financial crimes in Malawi.

2.1 Fraud

For the purposes of this report, fraud related crimes covered are of two dimensions:

- Public funds swindling scam, and
- Defrauding of private organisations.

Government continues to lose a lot of funds through unscrupulous public officials who connive with some service providers to pay for fictitious goods and services. Such officials also engage in tender rigging with the aim of getting bribes from service providers. Tender rigging, generally, is a conspiracy to award tenders to relations or associates with the view of getting some payment in return as a token of appreciation. Tender rigging is difficult to ascertain because of the secrecy that surrounds the awarding of contract and the way in which payments are made for the services and goods.

Apart from the public officials, there are certain individuals who use their influence due to their positions in the private organisations such as companies and non-governmental organisations to engage in fraud syndicates as well as abuse of office. Usually, illicit proceeds from these scams inevitably find their way into the financial system where these individuals try to disguise the origin of the proceeds through numerous transactions and entities. Case studies in this report illustrate this phenomenon.

2.2 Tax Evasion

The MRA indicated that the most prevalent cases under their investigations were under-invoicing, smuggling, suppression of sales, claiming non-allowable expenses, claiming non-allowable VAT, non-remittance of withholding tax, and undervaluation of imports. Through analysis, the FIU has also established that there is a trend whereby some individuals and companies use private or personal bank accounts to evade tax.

2.3 Trade-based Money Laundering

There are some individuals and companies who flout Exchange Control Regulations for purposes of externalising funds to various jurisdictions such as Mauritius, South Africa, India and the United Kingdom.

Through collaboration among the FIU, Reserve Bank of Malawi (RBM) and MRA, syndicates have been uncovered involving fictitious and over-inflated invoices. Analysis by the FIU has also uncovered payments for goods and services rendered in Malawi but being made in a third jurisdiction.

3.0 Money Laundering Case Studies

3.1 Money laundering through tax evasion

The most prevalent cases under tax evasion were under-invoicing, smuggling, suppression of sales, claiming non-allowable expenses, claiming non-allowable VAT, non-remittance of withholding tax, and undervaluation of imports. However, for the purposes of this report emphasis was on cases which involved the use of financial system to disguise ill-gotten gains.

Egmont group of FIUs champions the very same fight against tax evasion and money laundering. Other schools of thought have in the past suggested that one cannot launder funds generated in own business. However, the FIU took a simplistic and logical view that if subjects evade tax then they could generally be rooted in handling tainted money even from other sources. Tax evasion is not a victim-less crime. The money involved belongs to the state.

Case Summary:

<i>Offence</i>	<i>Tax Evasion and Money Laundering?</i>
<i>Customer</i>	<i>Businesses and individuals</i>
<i>Product</i>	<i>Cheques</i> <i>Cash</i>
<i>Services</i>	<i>Accounts (Savings & Current)</i>
<i>Channel</i>	<i>Face to Face</i>
<i>Indicators</i>	<ul style="list-style-type: none">• <i>Large cheque deposits in personal accounts</i>• <i>Activity in account not matching with declaration</i>

Case 1 -Tax Evasion - Use of personal bank account for business purposes.

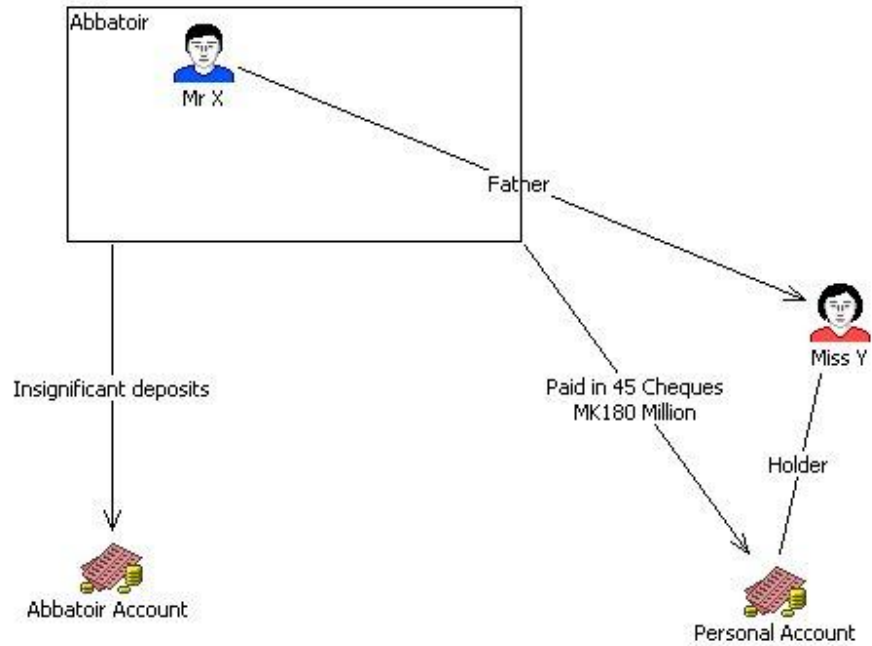
Many businesses in Malawi operate as sole traders. Businesses are encouraged to open business bank accounts. However, some businesses use personal bank accounts in order to avoid remitting tax from their turnover. The malpractice was mostly common among sole traders and other private limited liability companies.

Such businesses deposit significant parts of their proceeds in their personal accounts or those of associates or relatives. The personal accounts operate in an unhindered manner because of the grey area within the local financial system dynamics.

There was a case which the FIU analysed that involved the phenomenon just explained above. The analysis revealed that a father (Mr. X) and daughter (Miss Y) were involved in diverting proceeds of a legitimate business to a personal account between January and July 2009. The father was a managing director of a successful abattoir in the Malawi. He was depositing proceeds of his business in his daughter's personal account. The deposits that were made included over 45 cheques totaling MWK180 million. The daughter was not a registered tax payer and the business books showed little activity, hence MRA collected very little in taxes.

After FIU analysis, investigations ensued and the subject pleaded guilty to tax evasion and subsequently paid MWK35 million to MRA.

Below is a chart showing how the scheme worked.



3.2 Laundering of money stolen from Government

Through analysis of transactions provided by financial institutions, the FIU has established that there are some crooked individuals who use false names for purposes of disguising proceeds of crime using the financial system.

Case Summary:

<i>Offence</i>	<i>Fraud and Money Laundering</i>
<i>Customer</i>	<i>Individual Business</i>
<i>Product</i>	<i>Cheques Cash</i>
<i>Indicators</i>	<ul style="list-style-type: none"> • <i>Business activity inconsistent with account opening/KYC</i> • <i>Large cheque deposits</i> • <i>Smurfing</i> • <i>Use of low level ID</i> • <i>Use of false identity</i>

Case 2.1 - Laundering money stolen from Government using false names and accomplices in financial system

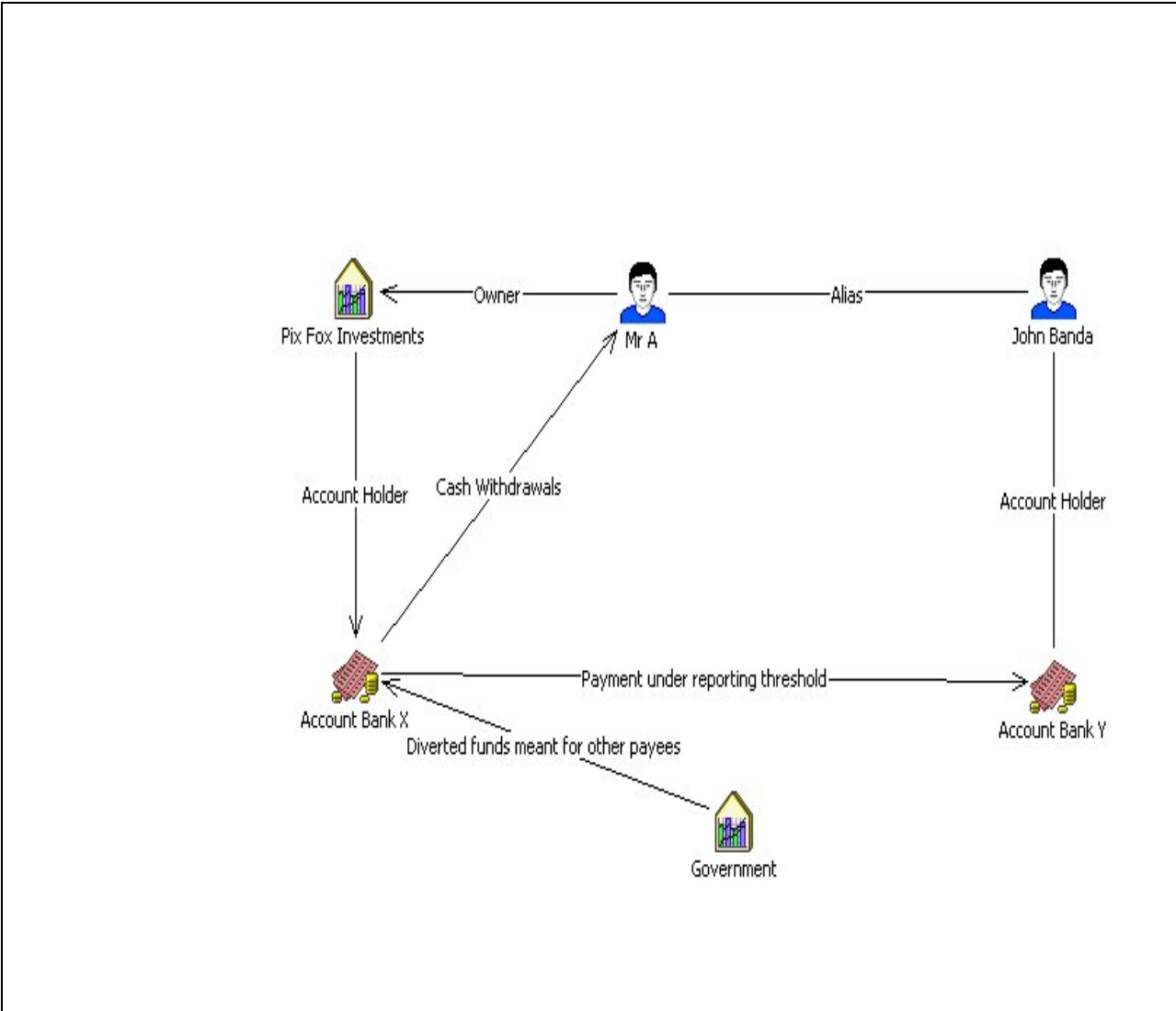
A suspect (Mr. A) had been having unusual activities in his personal account with bank X. The FIU's analysis uncovered Mr. A's fraudulent activities that took place between 2010 and 2011 involving over MWK32 million. Mr. A identified himself as John Phiri in bank X and Jack Banda in bank Y. The subject had identified himself as a director of Pix Fox Investments, which was a duly registered company.

Government cheques were fraudulently processed by the Accountant General's Department (AGD) payable to public and private entities. The cheques were collected from the AGD's office by individuals purporting to be employees of the beneficiary organizations but these individuals did not provide legitimate identities.

The government cheques were being deposited into an account of Pix Fox Investments in Bank X. This business, which was based in Blantyre, was owned by John Phiri. He had another account at Bank Y in Lilongwe. He used a letter from the District Commissioner as his identification document to open a personal account at Bank Y where he presented himself as Jack Banda. He also submitted a certificate of registration from the Registrar of Companies and a company identity card purported to have been issued by Katakwe Investments. The reference letter was signed by Jimmy Banda, his brother, in his capacity as Director. The dates of birth for John Phiri and Jack Banda and physical appearances on ID photos submitted to Bank X and Y were similar.

The suspect was collecting government cheques whose payees were other state bodies and private companies including banks. With the aid of bank X staff, the Government cheques were presented for clearing at the central bank duly bearing the official stamp of Bank X despite that fact that the beneficiaries did not have an account with Bank X. He was then fraudulently depositing the money equivalent to the government cheque in his account in Bank X. The scheme was well thought out through use of Bank X staff to conceal the payee name by stamping the cheques at the critical payee space. His accomplices at Bank X would then split the cheque amount under the reporting threshold of MWK1 million. The drawer and cheque number input in the system were bogus but the total was backed by real money stolen from Government through this means.

The suspect would then draw cheques in favour of his alias in Bank X. The funds would then be withdrawn as cash.



Case 3.3 Defrauding of Government through payment for undelivered goods and services.

Case Summary:

<i>Offence</i>	<i>Fraud, Corruption and Money Laundering</i>
<i>Customer</i>	<i>Businesses and individuals</i>
<i>Product</i>	<i>Cheques Cash</i>
<i>Services</i>	<i>Accounts (Savings & Current)</i>
<i>Channel</i>	<i>Face to Face</i>

<i>Indicators</i>	<ul style="list-style-type: none"> • <i>Large cheque deposits in personal business accounts</i> • <i>Activity in account not matching the known business trends of similar business types</i> • <i>Multiple cheques deposited from same drawer drawn on similar dates.</i> • <i>Use of a dormant account</i>
-------------------	--

The FIU's analysis uncovered a syndicate where public officials at a certain government department connived with a business owner to make payments for goods which were never supplied.

Four cheques totaling MWK 12 million were deposited in an account of a family business A. One of the directors of the business had once worked at the government department. Analysis of the account showed that there was insignificant activity prior to the deposit of the cheques. The cheques, all in a same series of sequence, were deposited on the same day. Immediately after clearing, the owner of company A withdrew almost the whole amount, save for MWK900, 000.00. The bank enquired about the transaction and did not get satisfactory response hence filed an STR to the FIU.

Analysis by the FIU pointed to a suspicion that payment procedures at the government agency and the paying authority could be flawed. This was later corroborated through investigations by law enforcement on the government agency. The account of the said family business was getting funds as payment for goods that were never supplied. The case was ongoing and suspects are on bail as at the date of publishing this report.

Loss of government funds also happens because of bid rigging and abuse of system, but these are difficult to uncover due to concealed nature of the payments and benefits. However, net worth analysis often times unearths concealed income.

3.4 Fraud and Money laundering through a series of companies

Case Summary:

<i>Offence</i>	<i>Fraud and Money Laundering</i>
<i>Customer</i>	<i>Businesses and individuals</i>
<i>Product</i>	<i>Cheques Cash</i>
<i>Services</i>	<i>Accounts (Savings & Current)</i>

<i>Channel</i>	<i>Face to Face</i>
<i>Indicators</i>	<ul style="list-style-type: none"> • <i>Large cheque deposits in personal accounts</i> • <i>Activity in account not matching with declaration</i> • <i>Series of transfers and deposits in various accounts</i>

Analysis by the FIU revealed that two individuals connived to defraud a big retail company. One of the persons involved was a financial controller of the retail business and the other was a worker at a government agency. The public worker, whose salary was MWK65 000, had several companies and businesses registered in his name. One of the companies, company X, was an official supplier to the retail company. Over a period of two years the financial controller, owing to weak controls as well as his authority at the retail company, regularly facilitated payment of cheques to company X as payment for goods which were however never supplied. Another company belonging to the public sector officer later became a recipient of these illicit funds through cheque and cash deposits. Despite running 'successful' businesses, the public worker maintained his position at the government agency.

Other funds from this scheme were withdrawn or transferred to the public workers personal account and other businesses. The public officer was meanwhile accumulating wealth at an unprecedented speed and building establishments in his home area.

Further investigations revealed that approximately MWK103 Million was siphoned from the retail giant. Civil Case has commenced on the Financial Controller to repay the money and Criminal Case is ongoing and both subjects are on bail

3.5 Use of foreign remittance for capital flight

Case Summary:

<i>Offence</i>	<i>Externalization of funds</i>
<i>Customer</i>	<i>Businesses and individuals</i>
<i>Services</i>	<i>Telegraphic transfers/ remittances, external travel</i>

	<i>allowances (forex)</i>
<i>Channel</i>	<i>Face to Face, electronic</i>
<i>Indicators</i>	<ul style="list-style-type: none"> • <i>High-value cash deposits</i> • <i>International funds transfers made soon after cash deposits</i> • <i>Third party individuals making large cash deposits in favour of the subjects</i> • <i>Multiple customers sending money to same beneficiary</i>

Early 2011, the FIU assisted the Malawi Revenue Authority (MRA) to uncover a scam on importing used machinery from Turkey at a very inflated cost price. The importer declared to authorities that the machinery was worth US\$4 million. A bank made US\$750,000 as part payment for the used machinery. Upon arrival in the country, inspection of the machinery was found it to be obsolete. Investigations established that it was part of the machinery off boarded equipment from privatisation of state companies in that country.

Investigations by the MRA in conjunction with the FIU and RBM established that the international market value of a brand new machinery of similar nature was US\$600, 000 only. Further payment for this machinery was therefore halted.

3.6 NGO Director illegally used charity funds for personal gain.

Case Summary:

<i>Offence</i>	<i>Fraud and Money Laundering</i>
<i>Customer</i>	<i>Businesses and individuals</i>
<i>Product</i>	<i>Cheques Cash</i>
<i>Services</i>	<i>Accounts (Savings & Current)</i>
<i>Channel</i>	<i>Face to Face</i>
<i>Indicators</i>	<ul style="list-style-type: none"> • <i>Large cheque deposits in personal accounts</i> • <i>Activity in account not matching with declaration</i> • <i>Regular inexplicable travel allowance</i> • <i>Use of spouse in official business</i>

A director of an NGO liberally used funds meant for the institution’s operations to fund activities for a lavish lifestyle. An STR was lodged by a financial institution after noting that the subject was regularly withdrawing funds for external travel to meet suppliers. The director also involved her spouse. The subject could not satisfactorily explain the external travel allowance and the involvement of the spouse.

Analysis by the FIU identified that the original benefactor of the NGO prepared a constitution which offered no oversight in terms of board or trustees. This clearly meant the director was the final unquestionable authority in terms of the use of funds. This was a typical case of abuse of office.

3.7 Trade based money laundering

Case Summary:

<i>Offence</i>	<i>Money Laundering</i>
<i>Customer</i>	<i>Businesses and individuals</i>
<i>Product</i>	<i>Cheques Cash Forex transfers</i>
<i>Services</i>	<i>Accounts (Savings & Current)</i>
<i>Channel</i>	<i>Face to Face Phone Correspondence</i>
<i>Indicators</i>	<ul style="list-style-type: none"> • <i>Large cheque deposits in personal accounts</i> • <i>Activity in account not matching with declaration</i> • <i>Excessive forex remittances</i> • <i>Fake MRA documents</i>

The FIU received a suspicious transaction report on Companies A, B and C on illegal externalization of forex claiming to be importing goods. The three companies, with their associates, were externalizing funds to various destinations in the world on pretext of importing goods. Analysis by the FIU, with the help of foreign FIUs, found out that these companies were mainly sending funds to companies of James Banda (fictitious name), a resident and citizen of Malawi. Furthermore, owners of companies B and C claimed to be citizens of a foreign country X. The passports they submitted when opening bank accounts were sent to the FIU of country X for verification. Country X’s FIU run a

search of the identities and found out that the passports submitted to Malawian Immigration authorities and banks were fake.

An investigation by banks could not locate business premises of Companies A, B and C at the declared physical places in bank documents. Businesses around the declared physical locations said that they had never heard of such companies. The direction that these companies indicated to the banks was fictitious and non-existent. This further shows that these were “briefcase or fake” entities set up to facilitate illegal remittances of foreign exchange.

The FIU, in conjunction with MRA, found out that the documents used by Company A, especially, to externalize forex were forged. All the forex remittances were made based on fake customs documents, which implied that the alleged imports were never made. The forged documents, plus non-existence of business premises, proved that the purported imports were also fake.

In one instance, an invoice showed purchase from one Company of James Banda, based in Country C, of big items like fridges, computers, and other electrical items which ordinarily needed a business place for storage and display. Since the companies did not have physical place of operating this proved to be a fictitious invoice.

An order was made to freeze the accounts of the three companies and the associates. It can safely be assumed that James Banda’s accounts and those of his various businesses were being used as the layering point in these transactions.

3.8 Capital flight through agents based abroad

Case Summary:

<i>Offence</i>	<i>Externalization of funds</i>
<i>Customer</i>	<i>Businesses and individuals</i>
<i>Services</i>	<i>Telegraphic transfers/ remittances, external travel allowances (forex)</i>
<i>Channel</i>	<i>Face to Face, electronic</i>
<i>Indicators</i>	<ul style="list-style-type: none"> • <i>Numerous international funds transfers</i> • <i>Payments for diverse goods and services made to same beneficiary</i> • <i>Employing foreign nationals</i> • <i>Use of third parties to conduct business transactions abroad</i> • <i>Holding bank accounts with numerous local banks</i>

	<ul style="list-style-type: none"> • <i>Importation of locally available goods and services</i> • <i>High volume (aggregated value) of international funds transfers</i>
--	--

Analysis by the FIU and ACB resulted into uncovering of over-inflation of invoices by using third parties to procure goods, some of which were locally found.

Company X in Malawi was importing a raw material from Turkey and the Far East. The company did not buy the commodity directly but used an agent in the United Kingdom. The agent happened to be related to a Director of company X. The agent was responsible for procurement of various commodities on behalf of company X in Europe and the Far East. The company in question was also procuring spare parts for its machinery using the same agent. Analysis of the information from the banks indicated that the company had several accounts with local banks which they were using to facilitate foreign payments. Analysis also identified three prominent companies that were receiving payments from Company X.

Suspicious transactions reports were filed to the FIU and analysis of financial transactions and historical data on world price index and other sources pointed to the fact that the agent was over-inflating the prices of commodities by almost double. Preliminary investigations revealed that company X had fraudulently sent over US\$3.5 million abroad using this scheme. Half of these funds were deemed to have been externalized illegally. Investigations were at an advanced stage at the time of publishing this report.

4.0 Conclusion

This report is very important. It has come out at a time when the country is consolidating its AML/CFT framework. Stakeholders are therefore being urged to be vigilant and make use of information from this report to combat criminal activities and prevent the perpetrators from enjoying proceeds of their crimes.