MONEY LAUNDERING TYPOLOGIES IN MALAWI

JUNE 2016

TABLE OF CONTENTS

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/Customer
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

FOREWORD

1. Under Section 11(2)(n) of the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Act (ML Act), the Financial Intelligence Unit is mandated to produce trends and typologies on money laundering and terrorist financing.

2. Pursuant to this mandate, the FIU conducted a second typologies study on Money Laundering, Terrorist Financing and other Financial Crimes. Like the previous report (Malawi Money Laundering Typologies 2011), this edition provides a comprehensive picture of the money laundering process. The case studies in this report provide a platform to identify new threats or refined old methods which criminals are using to launder proceeds of crime.

3. The report strengthens the fight against money laundering and terrorist financing by providing sanitized case studies as classic examples of the methods being used by the perpetrators of money laundering.

4. This study covers the period from January 2012 to December 2015, a time when the country experienced a major fraud scandal involving staff members in the public service and some business entities, commonly known as *cashgate*.

5. Typologies are generally methods or trends through which proceeds of crime are disguised by criminals to appear to be originating from legitimate sources. The proceeds from the predicate crimes are moved through financial institutions using various methods which are discussed later in this report. As you will notice in this report, the major methods used for money laundering during this period were public sector fraud, private sector fraud, tax evasion, trade-based money laundering, and use of cheques and wire transfers.

6. Case studies and other information used in this report are from the Law Enforcement Agencies (LEAs) and the FIU database. The case studies were sanitized for public consumption. The use of these case studies is duly authorized. The cases do not depict any person, natural or legal, living or dead. The report shows examples of how criminals are exploiting or attempting to

exploit Malawi's financial system to move their illicit proceeds of crime. The report is also providing a platform for exchange of ideas and lessons to be learnt in order to make informed decisions in handling matters that affect the country.

7. As Malawi is reeling from the effects of *cashgate* and other social ills, Government and all stakeholders must work together to find solutions to these challenges.

8. The role of the media and other players such as non-governmental organizations cannot be ignored. Sometimes the financial system may not generate all the reports for the FIU's analysis and in such cases the media has provided valuable information. The media has also assisted in enhancing integrity and transparency for exposing financial lapses and shortcomings in government financial management. The wide interest generated from media instills high public awareness about importance of integrity and transparency in the public service.

INTRODUCTION TO THE FIGHT AGAINST MONEY LAUNDERING AND TERRORIST FINANCING IN MALAWI

9. The fight against money laundering in Malawi is governed the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Act, 2006, and Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011. This Act also established the Financial Intelligence Unit as an autonomous central national agency responsible for receiving, requesting and analyzing financial information, and disseminating to competent authorities financial intelligence to combat money laundering and terrorist financing.

10. FIU Malawi is administrative in nature, meaning that it cannot investigate or prosecute matters relating to money laundering and terrorist financing. The Malawi FIU's core functions are to receive and analyze and disseminate to competent authorities disclosures of financial information in order to counter money laundering and financing of terrorism. The competent authorities to which the FIU disseminates information include the Malawi Revenue Authority, Anti-Corruption Bureau, Fiscal and Fraud Unit of the Malawi Police Service, the Directorate of Public Prosecutions and the Immigration Department. The application of intelligence and analysis techniques is one of the best ways of detecting and disrupting money laundering and the activities of terrorists and terrorist organizations. This report bridges the gap in terms of information sharing on trends being employed by criminals.

SUSPICIOUS TRANSACTION REPORTING

11. The Malawi FIU receives disclosures of financial information from financial institutions. The definition of financial institution under the Act is quite broad. It includes, among others:

- Banks
- Foreign Exchange Bureaus
- Microfinance institutions

- Insurance companies, including brokers & agents
- Money remitters
- Leasing & Finance
- Stockbrokers & portfolio managers
- E-money providers
- Designated Non-Financial Businesses & Professions (DNFBPs) which include:
    - Businesses dealing in real estate
    - Legal practitioners, notaries and accountants when they assist clients buy or sell real estate
    - Businesses dealing in precious metals and stones

12. The Minister of finance may at any time designate any sector as reporting institutions according to the perceived level of risk that the sector poses.

13. All financial institutions, as defined under the ML Act, are required to report suspicious transactions to the FIU.

14. Although all financial institutions are required to report suspicious transactions, the banking sector has been the primary source of information for the FIU due to its higher level of reporting obligation compliance than the other sectors. Efforts have been made to ensure that other financial institutions are reporting or are aware of the reporting obligations. This has, however, been done on a risk-based approach.

CONSEQUENCES OF MONEY LAUNDERING AND TERRORIST FINANCING

15. The government of Malawi is highly committed to the fight against money laundering and terrorist financing owing to the catastrophic consequences of both vices. Some of the consequences of money laundering include:

- **Undermining of legitimate private sector investments.** Money laundering undermines the legitimate private sector investments through the use of front companies to mask illegal activities. This in turn creates competitive inequalities whereby criminals eventually crowd out legitimate businesses because they can afford to charge low prices for their products/services since their profits are not necessarily from those businesses.

- **Weakening of financial institutions.** Proceeds of crime may be volatile as criminals may decide to move their investments elsewhere at any time and this may create liquidity problems for financial institutions.

- **Reputational damage.** Financial institutions rely on reputation for probity and integrity because they deal with other people's money. A financial institution found to have assisted in laundering money is shunned by legitimate businesses. The stiffest punishment for financial institutions aiding money laundering and terrorist financing is revocation of business license.

- **Difficulties in securing foreign direct investment.** A country that is friendly to money launderers can become an ideal financial haven and this compounds negative consequences of money laundering and terrorist financing. Developing countries, like Malawi, if allowed to attract dirty money or proceeds of crime as a short term catalyst for growth can find it difficult to attract the kind of solid long-term foreign direct investment that is based on stable conditions and good governance, and that can help them sustain development and promote long-term sustainable growth.

- **Erode a nation's economy.** Money laundering can also erode a country's economy by increasing the demand for cash, making interest and exchange rates more volatile, and causing high inflation.

- **Fuels corruption and organized crime.** Most disturbing of all, money laundering fuels corruption and organized crime. Corrupt public officials have the need to launder bribes, public funds (obtained through fraudulent means) and, sometimes, even development loans and grants from international financial institutions. Organized criminal groups need to be able to launder the proceeds of illegal activities. Terrorist groups use money laundering channels to get cash to buy arms and other goods and services. The social consequences of allowing these groups to launder money can be disastrous. Taking away the proceeds of crimes from corrupt public officials, purveyors of other serious crime and organized crime groups is one of the best ways to stop criminals in their tracks.

MONEY LAUNDERING PROCESS

16. Profit is the main reason for engaging in almost any type of criminal activity. The main aim of any anti-money laundering regime is therefore to take away profit from the crime. Usually, this process is multi-layered involving three stages; placement, layering and integration. These can be explained as follows:

Placement

17. During this phase, the proceeds derived from unlawful activities are placed in the financial system e.g. banks, casinos, forex bureaus, real estate agents, insurance firms, etc. There are a variety of ways in which the illegal proceeds may enter the financial system:

- direct depositing of money from crime proceeds into a bank
- exchange of currency into another;
- conversion into financial instruments (cheques, money orders);

- purchase of stock/ shares, purchase of security like insurance policies;
- mingling with legitimate funds;
- purchase of high value assets

Layering

18. This involves creation of complex networks/layers of transactions in order to create a distance between the criminal, source of funds and the transaction. For instance:

- reselling high value goods,
- wire transfers to several accounts/ other jurisdictions
- transfer to front/ shell company
- disguise transfer as payments of goods/services

Integration

19. This is where laundered proceeds are placed back into the economy in such a way that they re-enter the financial system appearing as normal business transactions. Examples are venturing into legitimate businesses and purchase of real estate or luxury assets.

20. However, money laundering does not need all three stages to successfully occur.

21. Terrorists and terrorist organizations also rely on money to sustain themselves and to carry out terrorist acts. Money for terrorist activities is derived from both legitimate and illegitimate sources. While terrorists are not greatly concerned with disguising the origin of money, their financiers are concerned with concealing its destination and the purpose for which it has been sent.

22. Terrorists and terrorist organizations employ techniques similar to those used by money launderers to hide their money. The main difference between

money laundering and terrorist financing is that sometimes terrorist financing involves laundering of legitimate funds. Money may be derived from well-known and legitimate businesses and may be channeled to terrorist organizations through foreign payments for goods and services. These acts may be aided by corrupt individuals in the financial industry who themselves may not be aware of the dire consequences of their actions. The criminal elements involved in terrorist financing try to distance themselves from the funds and terrorist activities. In Malawi, treasury departments within the banking industry are at a great exposure to this risk dimension. There is need to do enhanced due diligence on customers accessing foreign exchange products.

VULNERABILITIES OF THE FINANCIAL SYSTEM

23. As noted above, the primary source of information provided in this report is the banking sector. This report therefore considers vulnerability in the context of the banking sector. The banking sector is widely used by money launderers because it is the most commonly used financial system offering a variety of services. Further, the sector has a global network, is timely and convenient and can easily be used for all the three stages of money laundering, namely; placement, layering and integration.

24. The financial system is prone to money laundering and some of the issues that contribute to this vulnerability include, but not limited to, the following:

25. **Cash-based Economy.** Malawi is a 'cash based' economy; it is therefore not unusual for one to bring to the banking hall bags of cash for deposit or withdraw huge sums of money in cash. This is true for all other sectors as well. There are numerous examples of people purchasing high value assets in cash or purchasing other financial products in cash. This state of affairs makes it difficult for banks and other financial institutions to differentiate normal transactions from unusual ones. The *cashgate* scandal has opened a new dimension of vulnerability in terms of our system allowing business people to withdraw huge amounts of cash from banks. The debate about withdrawals of huge sums of money in cash rages on. There have been sentiments that there should be limits

as to the amounts that could be withdrawn in cash from the banks. Other measures considered include setting threshold of transactions that should involve other forms of instruments that have probity and an audit trail. The National Payment Systems Department of the Reserve Bank of Malawi is also exploring a number of initiatives to encourage usage of electronic payment systems in order to minimize cash transactions and provide audit trail for transactions. This would be for the benefit of oversight institutions like the FIU to be able to reconstruct transactions when and if need arises.

26. **Lack of national identification documents**. Malawi does not have a national identification system. The only reliable and verifiable IDs are driver's licence and passport. However, these ID types are issued upon need; for instance, when one wants to travel to other countries in the case of a passport. The absence of reliable IDs leads to banks opening accounts without sufficient identification documents. This is exacerbated by the fact that most Malawians do not have verifiable physical addresses. The lack of reliable IDs and verifiable physical addresses is a vulnerability that money launderers can exploit because they know they will not be traced.

27. **The size of the informal economy & the unbanked population.** According to a FINSCOPE, 2014 study, only 32% of the Malawian population has access to banking services. This means that 68% of the population transacts outside of the banking sector. The World Bank report of 2007 on Shadow Economies estimated the size of the informal economy in Malawi at 41.6%. The high level of the informal sector coupled with the cash-based nature of the economy makes it easier for proceeds of crime to be integrated into the rest of the economy without involvement of the financial system in the initial stages of the laundering process. Use of the financial sector may be unavoidable during later stages but money laundering would have already taken place by then. Financial institutions would be dealing with funds that have already been laundered and may not therefore detect them.

28. **Globalization.** It is now possible to transfer funds quickly across international borders, thanks to globalization. Criminals are therefore able to

move their funds quickly before banks and regulators can detect irregularities in the transactions. It is therefore important to fight money laundering in order to deter would-be offenders and established offenders from committing the predicate crimes and consequently laundering the money to distance themselves from the said crimes.

29. In recent years, the international community has become more aware of the dangers that money laundering poses in all these areas and many governments and jurisdictions have committed themselves to taking action. The United Nations and other international organizations are committed to helping in any way they can.

METHODS

30. Money laundering comprises methods by which criminals disguise the illegal origins of their wealth and protect their assets, so as to avoid the suspicion of financial institutions and competent authorities, and avoid leaving a trail of incriminating evidence. During the period under consideration, the most prevalent money laundering methods included:

- **Public sector fraud - *cashgate***
- **Use of fake cheques**
- **Use of personal accounts to evade tax**
- **Over-/under-invoicing of goods and services**
- **Use of bank cheques/transfers and third parties**
- **Use of alternative remittance systems – *Hawala***

Typology 1: Public Sector Fraud

31. Sophisticated fraud in the public sector continues to rear its ugly head. Public sector fraud in Malawi involves criminal elements within the sector and other people who exploit the system for their personal gain.

32. This fraud affects all Malawians because the funds involved are taxpayers' hard-earned money. Since most of the channels used to perpetrate fraud were uncovered nearly five years ago, criminals have become more sophisticated in that they are seemingly running a parallel public finance system. The criminals are producing fake documentation to deliberately deceive and exploit public expenditure lines which are primarily there for the benefit of genuine persons.

33. The FIU also uncovered fake cheques meant for destruction but found their way back into the financial system. These incorrect and dishonest payments are being made out to Small and Medium Enterprises (SMEs) and individuals as payments for goods and services. The SMEs and individual involved usually have direct links with the perpetrators at the office making out the payments. The SMEs and individuals involved have no business with Malawi government and have neither rendered any service nor delivered any goods.

34. Bank accounts of companies and individuals are being used to place illegitimate funds into the financial system after which the money is then withdrawn in form of various instruments or moved around the financial system. Criminal elements are sometimes using unwitting individuals to receive payments in return for a cut on the proceeds once the funds have been withdrawn. In some cases, some front companies are being used to create distance between the real criminal elements and the illicit proceeds.

35. The FIU relies on Suspicious Transaction Reports (STRs) and Large Currency Transaction Reports (LCTRs) received from financial institutions as some of the platforms that help uncover the syndicates and other irregular activities in government.

Fraud involving the Integrated Financial Management Information System (IFMIS)

36. The Integrated Financial Management Information System (IFMIS) is the accounting software that the government of Malawi uses for managing public funds. All government ministries, departments and agencies (except district assemblies and other selected departments such as health centres) process their payments through this system which is centralized at the Accountant General's office in Lilongwe. Treasury Cashiers (South and North), which are online with the Accountant General's Office, handle payments in the southern and northern region.

37. The IFMIS was designed in such a way that it separates users' operational powers (user rights) at different stages involved in the generation of a payment. Users at each stage have specific tasks to perform at, and only at, that level, say at the stage of uploading funding, preparing vouchers, approving vouchers, or printing cheques. Then, there is a totally separate group of cheque signatories, which is not party to the payments generation process above.

38. Some selected accounts officials in all government institutions from Accounts Assistant level up to senior officers are involved in the operation of the IFMIS, which is an EPICOR based computer network.

39. Information Communication Technology (ICT) personnel assist in creation of users on the network and the System Administrator assists in giving users access to the EPICOR. The user is given a unique user name and he or she creates a password of his or her own choice, which is only known to him or her. The ICT personnel do not know the passwords of the users and cannot perform any payment operation, as they do not have such rights.

40. Payment is initiated in the IFMIS when there is a legitimate vendor and the payment can only be in favour of that vendor.

41. Once an accounts official has initiated a payment operation in the IFMIS, he or she cannot delete it. Deleting the operation requires having access to the

IFMIS server. Only ICT personnel have access to the IFMIS server. But they can only delete that operation after being given the user password of the operator.

Case Study 1.1: Fake funding and Generated Payments

Between 1st April and 30th September 2013, some accounts officials in Lilongwe at some four ministries in connivance with some ICT personnel uploaded fake funding and generated payments amounting to MK6.9 billion (US$15.5 million) in favour of some 39 businesses (vendors) for goods and services that were not provided. The criminal network involved some selected legitimate suppliers of goods and services, mostly construction companies.

When the payments were finally processed, the suppliers got the funds withdrawn from banks (in cash) soon after the cheques were cleared, thereby making the withdrawals trend at the commercial banks to swell up significantly. For example, between 30th August and 6th September 2013, a whooping MK2.3 billion (US$5.2 million) was withdrawn from the banks in cash. On 5th September 2013 alone, there was a whooping MK827 million (US$1.9 million) total withdrawals from the banks. Once the suppliers withdrew the funds, they handed over a considerable part of the funds to some accounts officials mostly in cash, while retaining a certain percentage.

A total of ten banks were used by the criminals to defraud government with 104 cheques at play in this scam. These were signed by six signatories. One signatory alone signed 96.2% of the 104 cheques.

The aim of the criminals was to defraud the Malawi Government. The users used real user names. Once the users completed their transactions in the IFMIS, they deleted them from the IFMIS server with the assistance of ICT personnel. And once deleted, the transactions could not be visible again in the IFMIS. The system suppliers, however, were later able

to trace the deleted transactions through a remote backup server. This has now been coined as the 'cashgate' scandal.

The suppliers and the accounts officials involved were later arrested on theft and money laundering charges. So far the courts of law have convicted a considerable number of suspects in the concluded *cashgate* cases. The other cases are ongoing at the courts of law.

Typology 2: Use of Fake Cheques

42. One other emerging trend is crooked individuals starting up a business with a similar name to an existing organization or business with an intention to divert cheques. The FIU has observed that these individuals are colluding with staff from organizations/businesses they target in order to have access to cheques which are then altered to fit for deposit in their accounts.

43. This on paper appears to be simple fraud, however, it must be noted that the scheme is very elaborate as the perpetrators have all the patience to wait for some time before enjoying the proceeds of crime.

44. These new techniques are particularly detrimental to businesses that have high volumes of merchandise with cheques and cash seemingly coming in from everywhere. These businesses can be targeted by criminals using stolen and forged cheques.

Case Study 2.1: Diverting Cheques to an Illegitimate Company

Mr. G registered a business with a name similar to a trendy technological company in Blantyre, Mzansi Technologies. Mr. G's company name 'Mzanti Technologies' was registered as a deliberate ploy to defraud the original company of its funds. Mr. G went on to open an account of the business in early May 2013 with Bank M. When opening the account, it was indicated that Mr. G was a sole proprietor and that he is in the

business of selling electronic gadgets, which is also Mzansi Technologies' business line.

On 27 May 2013, three cheques were deposited into the M bank account belonging to Mr. G's Mzanti Technologies, drawn on three different banks (Bank B, Bank S and Bank M) by purported clients. The bank personnel noted that there were alterations on the cheques especially the name 'Mzanti'. The bank was convinced that the cheques were originally drawn for Mzansi Technologies, but were altered to read Mzanti Technologies.

Analysis established that the accountant at Mzansi Technologies, Mr. X. connived with Mr. G to alter and divert cheques meant for Mzansi Technologies to Mzanti Technologies. It was also found that the Mzansi Technologies Accountant was in possession of deposit slips for Bank A where the cheques were originally supposed to be deposited with a forged bank stamp to reflect that the cheques were deposited in the bank account A in order to dupe his employer, Mzansi Technologies.

Mzanti Technologies owned by Mr. G opened the account at Bank M to collude with Mr. X, the Accountant to defraud Mzansi Technologies through alteration of cheques meant for Mzansi Technologies.

Both Mr. G and Mr. X were arrested on various charges. They are both out on bail answering to charges laid on them.

Red Flags

- Registration of a business name similar to an established and successful business.
- Depositing of defaced cheques or other instruments.
- Accepting high value cheques for a new business with no known experience or history.

Typology 3: Over and Under-Invoicing of Goods and Services

45. Trade-based Money-laundering is another area that is permeating the Malawi economy with huge losses to the economy. This is the major source of Illicit Financial Flows (IFF) out of Malawi. Trade-based money laundering is the process of disguising the proceeds of crime through the use of what appear to be legitimate trade transactions. This is usually achieved by misrepresenting the price, quantity or quality of imported or exported goods. In Malawi, examples of trade-based money laundering include over- or under-invoicing of goods and services. The key driver of this technique is misrepresentation of the price of goods or services in order to transfer additional value between an importer and exporter. Basically, the importer in Malawi colludes with a supplier in another jurisdiction to over-charge on the invoice in order for the additional value to remain in that jurisdiction or transferred elsewhere for the importer. Some of the cashgate cases had characteristics of this nature for the purchase of high value items for security establishments.

46. Cases under trade-based money laundering are perpetrated by both existing large businesses as well as new entrants in the market. The scale of the damage caused by new entrants cannot be underestimated. The volumes of 'trade' under this scheme are very huge and the potential losses run in hundreds of millions of Kwacha.

47. Usually, the new entrants register businesses and open bank accounts while developing a persona that they are very big businesses. Large cash deposits are made into these accounts and once the balance has reached an amount they wish to externalize, they make application for foreign exchange using doctored documents. In order for the perpetrator to keep the rouse going, they keep a certain percentage of the funds within trading range.

48. Under-invoicing technique is employed by exporters who set very modest prices for their goods in order to transfer the difference to the benefit in another jurisdiction. Both over- and under-invoicing are detrimental to the foreign exchange regime as well as tax collections by the Malawi Revenue Authority.

49. Under trade-based money laundering, criminals also use multiple invoicing of goods and services. This technique involves issuing more than one invoice for the same transaction thereby justifying multiple payments. Companies have multiple bank accounts in the financial system and they simply employ several financial institutions to make these additional payments and this makes these transactions even harder to detect. The Reserve Bank of Malawi has measures to curb this malpractice but it must be noted that trade finance is more document intensive than many other banking activities. It is more susceptible to documentary fraud, which can be linked to money laundering and terrorist financing. This fraud is perpetrated with the use of official-like documents from the Malawi revenue Authority and freight forwarding agents.

Over-valuation of imports for capital flight

50. Established big businesses with suppliers and sister companies overseas are either over-invoiced by the suppliers. Once an invoice is paid by the company through their bank, the supplier deducts his actual due amount and transfers/pays the difference into an account elected by the company paying the invoice. Conversely, for businesses with sister companies overseas, the local company then under-invoices the sister company. This enables the local company to keep illegal reserves offshore while at the same time reporting under-performance to reduce tax liability. Some companies have also engaged in raising working capital through phantom loans from their sister companies. This scheme involves real money being invested in the local business in infrastructure and the company is allowed to repatriate foreign direct investment (FDI) capital with interest.

Case study 3.1: Over-Valuation of Imports for Capital Flight

Four companies, S, T, B and M opened bank accounts with Bank C within weeks of each other. One of the companies, M, was originally from Jurisdiction X and was purportedly the supplier of goods to the other three companies. Companies S, T and B were recently registered

as sole proprietorships and had no trading history prior to the opening of the accounts at Bank C. The bank did not verify the veracity of the businesses and verifications were not made as regards to the declaration on of the extent of their trading. During the period August 2012 to June 2013, companies S, T and B made over 200 large cash deposits in their respective accounts. All the four companies had declared that they were trading in salt. Once a considerable deposit was made in an account, the owner of the company would then produce an invoice from company M in jurisdiction X and request the bank to pay for the product to another company Y in jurisdiction K. During the period under review, the companies externalized over K4billion (US$8.9million) out of Malawi. Enquiries in jurisdiction K showed that Company Y was registered as dealing in electrical appliances and nearly all the sums that were received from Malawi were sent to various jurisdictions.

Investigations by Law Enforcement Agencies established non-existence of the purported business premises of the subjects. All the subjects, who are of Asian origin, have since fled the country.

Red Flags

- The size of the shipment appears inconsistent with the scale of the exporter's or importers regular business activities.
- The type of commodity being shipped appears inconsistent with the exporter's or importers regular business activities.
- The customer directs payment of proceeds to an unrelated third party.

Case Study 3.2: Under-valuation of Exports and Over-valuation of Imports for Capital Flight

A naturalized Malawian, (Originally from Burundi) had two companies, A and B. Company A dealt in produce while company B in hardware items. Between the years 2009 and 2013, the subject, through Company A, would buy produce, mainly groundnuts, and export to East African countries. Company A allegedly exported over 100 tonnes of groundnuts during the period in question. The subject feigned ignorance of the requirement to fill in Currency Declaration Form (Form CD1) and reconcile proceeds of his exports once he has been paid. The Currency Declaration Form is legally required foreign exchange / currency control document (Exchange Control Act) that must be submitted by the exporter's commercial bank on behalf of the exporter to the Reserve Bank of Malawi (RBM) for any export valued at more than 5000 USD.

The subject alluded that he had an agent who did the paperwork on his behalf and had no clue of how the produce left the country. Proceeds from the sale of the produce were allegedly being sent to the Far East Asia where the subject was allegedly procuring his hardware merchandise. There were no documents to support this claim. Initial analysis showed that the value of the export proceeds were far more than what was purportedly being declared as imports value paid for the hardware items.

The subject was assessed for tax obligation and he has since paid his liability and accompanying penalties.

Red Flags

- Foreign or naturalized national operating a predominantly local business.

- Type of commodity being shipped inconsistent with the exporter's known capacity.
- Non-remittance of export proceeds.
- Non-compliance with exchange control regulations.

Typology 4: Use of Personal Accounts to Evade Tax

51. There are cases where a business person properly registers a business but chooses not to open a business account in the name of the business, instead the account is opened in his or her personal name. All the proceeds from the business are deposited into the personal account. This is particularly difficult for the authorities to assess the tax obligations of the business because the account is not in the name of the business.

52. In addition, foreign nationals are required to possess a Business Resident Permit (BRP) in order to do business in Malawi. They are also allowed to jointly register a business and obtain a BRP under the registered business name. However, in some cases though the business is jointly registered, the foreigners do business individually as can be observed in their bank account records. Though this may be done to facilitate the acquisition of the BRP, it is also a way of avoiding tax obligations because mostly the account of the registered business is less active than the personal accounts of the partners.

Case Study 4.1: Jointly Registering Businesses to Evade Tax

In January 2006, two Chinese nationals Mr. S and Mr. G jointly registered a business in the name of R Investments. In January, 2007, they obtained BRPs under the business name R Investments. They opened a business account in the name of their business R Investments at one of the local banks. Between April, 2010 and June, 2012, a total of MWK18million in cash was deposited to this account. These deposits were immediately

followed by cash withdrawals. However, each one of them maintained bank accounts in their personal names.

Mr. S. had two accounts in his personal name, one at bank A and another at bank B respectively. Between October, 2010 and November, 2011, he made cash deposits amounting to MWK9million at Bank B. No deposits were made into the account at bank A. Between 2011 to June, 2012, there was no trace as to where the deposits were going.

Mr. G. maintains two accounts in his personal name at Bank A and Bank B respectively. During the period December, 2011 to August, 2012, he made 84 cash deposits amounting to MWK16 Million at bank A and MWK1 million at Bank B. In total MWK17 million was deposited.

After analysis, the FIU established that the two nationals operated businesses individually and not jointly as registered. Furthermore, the business proceeds were being diverted into their personal bank accounts in order to evade tax.

The case was disseminated to MRA for investigations. Taxes were assessed and appropriate penalties were applied.

Red flags

- Consistently large deposits in personal accounts
- Lack of activity in businesses operated by BRP holders
- Non-payment of appropriate taxes

Case Study 4.2: Use of Personal Accounts to Evade Tax

Between 1st January, 2012 and 31st August, 2012, Mr. Y, who had a properly registered business in the name of X.X. Hauliers Limited, diverted proceeds of his business to his personal account. The total deposits amounted to MWK213 million. (Cash deposits of MWK189million and cheque deposits of MWK24 million). The cheque deposits were from well-known big business to which Mr. Y's company may have supplied goods or provided services. There was no trace of any bank account in the name of his registered business. There was no payment to the MRA from the account since the time of its opening in 2004.

After analysis by the FIU, the case was been disseminated to the Malawi Revenue Authority for investigations.

Red flags

- Consistently large deposits in personal accounts
- Lack of activity in businesses account of a legitimate business entity
- Non-payment of appropriate taxes

Typology 5: Use of Alternative Remittance Systems – *Hawala* System

53. Hawala or Hewala is an informal system for transferring money, especially across borders, in which local agents disburse or collect money or goods on behalf of friends, relatives, or other agents without legal protection or supervision, trusting that all remaining obligations will be settled through future transactions. It can also be referred to as an underground banking system based on trust whereby money can be made available internationally without actually moving it or leaving a record of the transaction. Terrorists are known to be extensive users of the system.

54. In Malawi, there has been an emerging intensity of this kind of system in many forms. Most players are small scale, dealing in a few hundred Pounds (GB£) or dollars (US$) to a few thousands in the said currencies. However, recently cases have emerged where significantly huge sums of money are being exchanged using this system. Ordinarily, a Malawian in diaspora finds an agent in Europe, USA or elsewhere who would link up with a local agent to disburse funds to friends or relatives at an agreed exchange rate. The practice is that a person in diaspora hands over cash in local currency at source (Europe € /£ or USA $) to an agent who is working on behalf of a principal based in Malawi who in turn hands over Malawi Kwacha to designated recipient in Malawi. Hawala works on the same principle as other remittance businesses such as MoneyGram and Western Union albeit unregistered and unregulated by prudential and AML/CFT supervisory authorities.

55. The worrying trend is that the system is also working in reverse where local businesses, usually foreign owned, are operating as agents, paying out funds in Malawi and getting foreign currency equivalent in their foreign accounts.

56. This practice is heavily detrimental to accounting for remittances from diaspora which could contribute to Malawi's foreign currency reserves. On the other extreme end, the practice is also denying Malawi of fair taxes that could be paid to Malawi Revenue Authority by the local businesses. Local companies

that are involved in under-declaration of turnover and profits to MRA are using this method to externalize their profits.

57. This practice is not regulated as the remittance agents are neither registered nor licensed.

Case Study 5.1: Illegal Hawala

Company X Ltd was a registered international company. In Malawi, it maintained a bank account with W Bank which was opened sometime in June 2013 with an initial deposit of K5, 000. According to the information declared when the account was being opened, the company was involved in import and exports, and hiring of heavy plant and machinery. Information gathered from other open sources indicated that the company, whose director, a foreign national of a SADC region country, based in United Kingdom was involved in financial mediation and informal international money transfers. The company also has a local director for the Malawi office.

There were huge cash deposits passing through the account from various sources which were followed by funds transfers.

Towards the end of June 2013 the account started receiving large cash deposits from various individuals. Between end of June and end of November 2013 the account received over K600 million as cash deposits. The cash deposits were usually followed by an immediate outward transfer of the funds to another bank account. The funds were usually transferred to an international NGO whose management had four nationals from the same country as the director of company X. According to records, the NGO's Directors/Trustees were European nationals. Once the funds were transferred into the NGO account there were numerous payments which were made out to beneficiaries. However, as compared to the funds that were received, it was a small

fraction which was paid out to this cause as a bigger chunk was yet again transferred out of the account.

The FIU's analysis showed that company X was externalizing huge sums of money from business person especially of Asian origin through a Hawala kind of system. The Asian business persons credited their local funds into company X account which in turn transferred the funds to the NGO which in return paid company X in foreign currency from the funds it got as an international Non-Profit Organization in a foreign jurisdiction. There was collusion between the owner company X and management of the International NGO to get favorable exchange rates for their foreign currency in Malawi while inadvertently aiding illegal externalization of currency and denying Malawi her fair share of taxes.

Red Flags

- High risk individual (foreign national) operating a local business
- Non-verifiable business interest.
- Rapid movement of funds (in and out of the account).
- Age of local Director inconsistent with magnitude of the business.
- Transfers to unrelated businesses.

Typology 6: Use of Bank Cheques/Transfers and Third Parties

58. Another emerging trend is the use of bank cheques to distance money launderers from proceeds of crime. Banks need to be aware of the potential for money laundering through the use of bank cheques. A bank issues a cheque made payable to a payee who elects to deposit the money into a seemingly third party bank account (Payment made to a third party by order of client). Many individuals and businesses have legitimate reasons for using bank cheques

for their transactions, but these cheques can be used to launder illicit funds or proceeds of crime.

59. Recently, there has been a rise in the use of bank cheques for transactions that would ordinarily have used other instruments such as own cheques to conduct the transaction. A bank cheque on paper is attractive to criminals as it shields the persons conducting the transaction. Bank cheques have a tendency of only showing up at the banks that has drawn the cheque. The receiving bank normally registers them as a deposit from another bank with the assumption that KYC and other due diligence measures have been duly done by the drawer bank. Money launderers may buy bank cheques to pay into their own accounts maintained at other banks.

60. Unwitting third parties may also be used to receive wire transfers and in turn order bank cheques or transfers to other banks for the benefit of the perpetrators. Usually, there may be a sudden, unexplained increase in account activity, both from cash and from non-cash transactions. An account may be opened with a nominal balance that subsequently increases rapidly and significantly. There may be numerous small or large incoming wires and/or multiple monetary instruments are deposited into an account. The customer then requests a large outgoing wire to another bank account. The customer may also order bank cheques in favor of a third party.

Case Study 6.1: Bank Cheques/ Transfers and Third parties

A local NGO based in one of the district in the central region through its account at Bank A (account for agriculture sector) transferred MK6million to Bank M with an order to credit the funds into the account of Miss C who was said to be involved in the business of buying and selling secondhand clothes.

Immediately after receiving the funds Miss C transferred MK5.5million to the account of X Distributors maintained at Bank M, in the same district as the NGO. She remained with MK500, 000 out of the MK6million transferred to her. X Distributors was owned by a Mr. P who was an employee of the NGO. X Distributors was involved in the business of distribution of liquor.

The transaction was suspicious because in normal circumstances the NGO would have issued a cheque directly to Miss C from its Bank A account. However, in this instance the NGO transferred funds to its account at Bank M who later deposited the funds in the account of Miss C. The immediate transfer of funds from Miss C to X Distributers meant that she was not the ultimate beneficiary of the funds. She only benefited MK500, 000 from the funds she received from NGO. The transactions were suspicious because the link between the source of funds, the NGO in Agricultural sector and the beneficiary liquor distribution did not make business sense. Mr. P used Miss C to siphon money from the NGO, his employer. Analysis showed that over a period of eight months, Mr. P received nearly K 30 million from the NGO through wire transfers to Miss C and others.

Red flags

- Funds transfer activity is unexplained, repetitive, or shows unusual patterns
- Rapid movement of funds (in and out of the account).
- Payments or receipts with no apparent links to legitimate contracts, goods, or services are received.
- Transfers to unrelated businesses

CONCLUSION

61. This report has highlighted money laundering methods employed by criminals during the period from 2012 to 2015 and these are: public sector fraud (known as *cashgate*), use of fake cheques, use of personal accounts to evade tax, over-/under-invoicing of goods and services, use of bank cheques/transfers and third parties, and use of alternative remittance systems (*hawala*). The report contains case studies and red flags to better explain the money laundering methods used.

62. Financial Institutions are in better position to detect and report suspicion of money-laundering and terrorist financing since they are usually in a business relationship with subjects of STRs. The above red flags may not be indicative to money laundering or terrorist financing if they are consistent with the clients declared and verified line of business or income.

63. The typologies, with their accompanying case studies, are for the purposes of illustration and keeping stakeholders aware of the emerging techniques and are not in themselves exhaustive or may not occur again or elsewhere in an exact fashion.