

A Financial Crime Free  
Malawi



# Typologies Report 2015- 2017

Financial Intelligence Authority

---

## Table of Contents

Abbreviations	2
Foreword	3
Introduction	4
Typology 1: Public Sector Fraud: Pensions and Gratuities	5
Case Study 1.1 Receipt of illegitimate allowances from Pension and Gratuities fund	6
Case 1.2 Receipt of illegitimate allowances from Pension and Gratuities fund	7
Typology 2: Trade based Money Laundering	8
Case Study 2.1 Use of fake MRA Form 12 document	10
Typology 3: Abuse of foreign Currency	11
Case Study 3.1 Use fake travel documents to claim foreign travel allowance	12
Case Study 3.2 Frequent use of one Travel Agent	13
Conclusion	13

## **Abbreviations**

FFU	Fiscal and Fraud Unit of Malawi Police Service
FI	Financial Institution
FIA	Financial Intelligence Authority
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
RE	Reporting Entities
STR	Suspicious Transaction Report
TF	Terrorist Financing

## **Foreword**

Money laundering (ML) is an offense that follows most criminal activities. The goal of the criminal in committing ML is to enjoy the proceeds of crime and to do this, criminals distance themselves from the crime and its proceeds through a number of schemes.

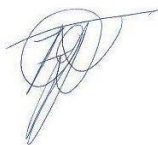
One of the Financial Intelligence Authority's (FIA) mandates is to conduct research on money laundering cases to identify similarities in how ML is accomplished and these become trends and typologies. Trends and typologies are generally methods used with the aim of defeating anti money laundering reporting measures in order for the criminals to enjoy proceeds of their criminal activities. Typology studies are undertaken to assist following up the money trail and identifying criminal proceeds.

Typologies can be used in different ways, two particular ways include; enabling Law Enforcement Agencies (LEAs) in preventing crime by taking away profit from crime. This would include using typologies to open up different avenues of investigation. Secondly, reporting entities (REs) use typologies to monitor accounts and transaction activity. Reporting entities may also use typologies to identify high risk customers, products and services, and improve in their overall risk management systems. This in turn improves the quality of suspicious transaction reports (STRs) submitted to the FIA.

In this 3<sup>rd</sup> typology report we have identified three major methods by which criminals are laundering and moving money to disguise their origins and integrate the money into the formal economy. The methods are: theft of public funds, illegal externalization of foreign exchange and abuse of travel allowances.

The compilation of these reports therefore remains a significant milestone in helping stakeholders in the country to develop and modify strategies and channel efforts towards combating the criminal activities as highlighted in this document. This will also help prioritize application of resource in the fight against money laundering.

Thank you for sparing time in reading this report. The fight against money laundering and terrorist financing and other financial crimes cannot be left to the Financial Intelligence Authority alone. Everyone needs to play their part to ensure a fair and level playing field for a financial crime free and prosperous Malawi.



**Atuweni Juwayeyi Agbermodji**

**Director General**

## **Introduction**

Criminals are continuously looking for opportunities to acquire profit from crime. The key mandate of the Financial Intelligence authority (FIA) is to prevent criminals acquiring profit from crime, and one way to do this, is to produce Typologies reports to inform stakeholders of various methods that criminals are using to launder, conceal proceeds of crimes as well as committing other financial and serious crimes.

In coming up with typologies reports, the FIA relies on the hundreds of thousands of threshold currency transaction reports (large currency transaction report) and reports of suspicious transactions it receives from Reporting Entities. The FIA analyses this transaction data to identify potential money laundering, terrorism financing and other serious financial crime.

The FIA shares its financial intelligence with local law enforcement agencies and international counterparts for use in their investigations and eventually prosecutions and other court actions. The reports received and analyzed by FIA assist in identifying relationships between individuals and their associates / networks, the movement of funds and patterns and trends of financial footprints.

This report contains various case studies that the FIA uncovered during the period 2015 to 2016. Almost all FIA intelligence analysis work relies on STRs submitted by Reporting entities. The value of high quality STRs cannot be overemphasized as these form the bedrock of intelligence gathering.

Stakeholders are urged to use the report to:

- Prioritize their efforts to ensure that high risk areas are given adequate resources to combat ML and TF.
- Conduct assessments to mitigate ML/TF risks that affect their organizations.
- Employ transaction monitoring systems that are able to detect suspicious transactions and thereby enhance reporting of STRs to the FIA.

The FIA reviewed cases in its database to identify trends of how criminals are operating within the Malawi financial system. These cases form typologies that have been used in this report. It should be noted that there are new typologies in the report as well as typologies that have been published in the previous reports. The old typologies are being discussed in this report, due to the fact that we have noted that criminals have built on the modus operandi identified in the old report. This therefore provides a clear understanding of why it is important for financial institutions to understand and use typologies.

## Typology 1: Public Sector Fraud: Pensions and Gratuities

In the previous report, we concentrated on Cashgate as the main activity under public sector fraud. Over the years we have seen growth in other frauds that involve the public sector. Our main area of focus in this report is Pensions and Gratuities.

The Financial Intelligence Authority uncovered a syndicate of Public Officers which defrauded the Malawi Government Pension funds by paying each other allowances from the Public Pensions and Gratuities fund account between 2012 and 2013. The proceeds from this crime were classified as fraud because public officers conspired to claim allowances from the fund which the Government uses to pay gratuities and pension to Civil Servants who either retired or died as provided for in the Malawi Public Service Regulations. In this case, individuals who are still working and obviously alive, have been illegally benefiting from the fund.

The syndicate was first uncovered around 2014/2015 through analysis of some bank accounts of Public officers which showed that there were frequent credits of funds from the Pensions and Gratuities fund into the officers bank accounts. There was significant turnover in the bank accounts of the public officers, comprising of Malawi Government allowances and self-cash deposits which are significantly higher than what is declared by the account holder on the accounts opening forms. In some instances some officers had their bank accounts credited with allowances every day. The credits of allowances were immediately followed up by ATM cash withdrawals, and at times the officers made cheque payments and import payments. In a typical money laundering scam, once funds are deposited in the accounts, the subjects transacted normally to create a façade that funds are legitimate.

The Public officers opened personal bank accounts with several banks which they used to receive the allowances. The officers prepared claim form for allowances and processed cheques which often were payable to Banks. The cheques were delivered to the banks with a list of names of the officers, amounts to be paid to each officer and their respective account numbers. On average one Public officer received over MK17 Million in allowances in a period of two years. The syndicate involved over 20 officers.

### CASE SUMMARY

<b><i>Offence</i></b>	<i>Theft by Public Servant and Money Laundering</i>
<b><i>Customer</i></b>	<i>Public officers</i>
<b><i>Product</i></b>	<i>Cheques and Instructions</i>
<b><i>Services</i></b>	<i>Accounts (savings and current)</i>
<b><i>Channel</i></b>	<i>ATM machines and face to face</i>
<b><i>Indicators</i></b>	<i>Frequent credits of funds in accounts described as Pensions and Gratuities Allowances paid from Pensions and Gratuities Account</i>

## Case Study 1.1 Receipt of illegitimate allowances from Pension and Gratuities fund

### Case Study 1.1 Receipt of illegitimate allowances from Pension and Gratuities fund

Mr. R. is employed in the Civil Service. He is entitled to receive MK15,000 in allowance per night if he travels outside his duty station on official duties. The officer maintained 9 Bank Accounts with various Banks. The officer declared the source of income as salary, allowances and income from transport business. An analysis of three Bank Accounts showed that between 20 July, 2012 and 1 October, 2013 the account received MK30, 700,000 in deposits described as Pension and Gratuities allowances.

Mr. R. maintains one of the three accounts with Bank G. The analysis traced a number of Malawi Government cheques payable to Bank G. Between 22 August, 2012 and 8 August, 2013 total amount of the cheques was MK27,000,000. From this amount Bank G credited Mr. R's account with MK8,100,000.

Analysis also showed that Mr. R's account at Bank F has turnover of MK23,240,241,055.34 from 20 July, 2012 to 31 July, 2013. From the amount, MK20,760,000 were direct credits described as allowances. This represented 89 percent of the total deposits into the account. MK2, 400,700 were cash deposits made by various individuals and MK6,400 was credit interest.

Further analysis showed that Mr. R's account with Bank E received MK1,755,000 in allowances from September, 2012 to 20 August, 2013. The allowances were described as Pensions and Gratuities.

In summary, between 20 July 2012 and 1 October, 2013 (438 days), Mr. R. received direct allowances from Malawi Government into his three bank accounts (Bank G, Bank F and Bank E) amounting to MK30,689,000. At his entitlement of MK15,000 per night the maximum he could have reasonably expected to receive in 438 days was K 6,570,000 (that is assuming that he has worked outside his duty station for the entire period). In other words, assuming that Mr. R worked outside his duty station continuously from 20 July, 2012 to 1 October 2013, a total of 438 days, he should have received a total of K 6,570,000 and NOT the K 30,689,000 which was against Government regulations.

## Case 1.2 Receipt of illegitimate allowances from Pension and Gratuities fund

### **And Case Study 1.2 Receipt of illegitimate allowances from Pension and Gratuities fund**

Mr. S is employed in the Civil Service. He is entitled to receive MK15,000 in allowance per night if he travels outside his duty station on official duties. The officer maintains 3 accounts with various Banks in Malawi. The source of income was described as salary, allowances and low scale transportation. Between 2012 and 2013 the total turnover in the accounts was MK32,310,000.

Analysis of Mr. S. account maintained with Bank X. revealed that the source of income in the account was described as salary. Between 2012 and 2013 the account received about MK17,002,500 in deposits. MK15,922,000 (94 percent) in deposits was described as allowances and MK1,080,000 (8 percent) as self-cash deposits.

Mr. S maintains another account with Bank Y. The source of income was described as salary. Between 2012 and 2013 the account received MK20,300,000 in deposits. MK14,452,000 in deposits was described as allowances representing 71 percent of the deposits. MK2,361,000 (12 percent) described as deposits by other people some of which were fellow officers and MK3,477,000 (17 percent) described as self-cash deposits.

Further analysis of Mr. S account maintained with Bank Z showed MK15,699,248.62 in deposits between 2012 and 2013. The source of income was described as salary and low scale transportation with a turnover of MK430,000. Of the deposits, MK4,347,965 was described as salary, MK7,209,282 as self-cash deposits, MK1,935,000 Pension and Gratuities and MK1,207,000 as deposits by other people.

In looking across the three bank accounts, 2012 was the year Mr. S. received more allowances from Government. He received MK24, 519,000. On average it would appear that he was receiving allowances of K67, 000 each and every day of the year. In 2012 there were two months (June-MK4, 310,000 and November-MK4, 362,500) in which he received more allowances. On average he received MK145, 400 per day in each of these two months. Furthermore, on 25th June, 2012 he received MK1, 085,000 in allowances scattered across the three accounts. Similarly on 12 and 15 November, 2012 Mr. S. received MK900, 000 and MK975, 000 in allowances respectively.

Even without looking at the actual circulars prescribing the government policy on allowances, applicable allowance rates and frequency at which Mr. S. received allowances from Malawi Government, the flow and trend of the allowances received is suspicious and does not make sense. For example, the receipt of multiple allowances on one day (25th June 2012), shows that the allowances were not justified and were received without following procedures. This was a typical case of theft and money-laundering.



## Typology 2: Trade based Money Laundering

In the previous Typologies report, trade based money laundering featured quite highly. The FIA has noticed that there is persistent activity where some businesses especially foreign owned are illegally externalizing foreign currency through import payments. In international trade, the applications for import payments are supported by fake Malawi Revenue Authority (MRA) Form 12, which is an Import Certificate. The fake Form 12 used in the transactions exist in the ASSYCUDA system and the stamps as well as signatures appeared to be genuine. However, the information on the Form 12 in the system was different. The forms in the system showed different importers, suppliers, value and type of goods, date of imports and duty paid. This means that the remittances were in violation of the Exchange Control Guidelines i.e Section II part 9.0 of the Operational Manual for Cross-Border Foreign Exchange Transactions. The remittances are destined for the same country in Asia.

The trend in the accounts is that the expected monthly/annual turnover declared was not consistent with the actual turnover in the bank accounts. The declared annual/monthly estimated income is significantly below the actual deposits and withdrawals passing through the account. Once huge deposits were made, they were immediately followed by externalization of funds the same day or within the next 2 days. The transactions do not make any business or economic sense. All accounts reviewed showed very high turnover inconsistent with what was declared during accounting opening leaving very low account balances. The behavior of the accounts is indicative of a possibility that the funds are just being ‘washed’ through these accounts. The funds could be proceeds of other illegal activities.

### Case Summary

<b>Offence</b>	<i>Illegal externalization of forex, money laundering, production of false documents, tax evasion</i>
<b>Customer</b>	<i>Sole proprietors (foreign owners)</i>
<b>Products</b>	<i>Cash, forex transfers</i>
<b>Indicators</b>	<i>Large cash deposits immediately followed up by application for import payment Activity in account not matching with declaration Frequent forex remittances Fake MRA Form 12</i>

## Case Study 2.1 Use of fake MRA Form 12 document

### Case Study 2.1 Use of fake MRA Form 12 document

In December, 2015, the FIA carried out investigations on 7 financial institutions to check import payments conducted from 2014 on a random sample of forex transactions carried out by each of the 7 Financial Institutions. In order to determine authenticity of the import documents, the FIA sent them to the MRA for verification.

The results were that the Form 12 used in the transactions exist in the ASSYCUDA system and the stamps as well as signatures appeared to be genuine. However, the information on the Form 12 in the system was different. The forms in the system showed different importers, suppliers, value and type of goods, date of imports and duty paid.

Transactions of total value of USD16.9 million (approximately MKW 12.0 billion) were found to have been supported by fake MRA Form 12 (form used to clear imports). This means that the remittances were in violation of the Exchange Control Guidelines i.e Section II part 9.0 of the Operational Manual for Cross-Border Foreign Exchange Transactions. Considering that FIA conducted this exercise using a random sample of the forex transactions, the actual amount of illegal forex transactions could be much higher. In addition, it is possible that other business entities are also involved in similar malpractices apart from the particular Asian ethnic nationals. These illegal forex transactions were noted in transactions carried out by two financial institutions. FI X (USD 16,521,832) and FI Y (USD 356,558).

The FIA study revealed that there were twenty two (22) businesses which were involved in the illegal forex transactions at FI X and that all of them were foreign owned.

## Case Study 2.2 Use of Fake MRA Form 12

### Case Study 2.2 Use of Fake MRA Form 12

X and Y maintain business and personal accounts with Financial Institution Z. The Account opening forms are not completed in full as some files do not indicate the expected annual turnover. In the files where the expected annual/monthly turnover is indicated it does tally with the turnover in the accounts. The turnover in the accounts is far much more than the declared turnover.

The two customers X and Y also appear to be using personal accounts to conduct business forex transactions. These two customers also used their Temporary Export Permits (TEP) in opening their business accounts instead of their Business Resident Permits (BRP). Further to this, there are no employment documents on their files to show whether the two are employed.

In both X and Y's bank accounts, huge deposits were made and immediately followed by externalization of funds the same day or within the next 2 days. The transactions did not make any business sense. From January, 2014 to November, 2015 X and Y externalized US\$2,653,026 and US\$1,442,190 respectively in the form of import payments. Some forex remittances were made years after the goods were alleged to have been received in the country. For instance in relation to customer X and based on the Form 12 that supported transaction for import payment of USD224,950.00, the goods were alleged to have been registered for Custom and cleared with MRA in 2011 yet the import remittance was made in mid 2014.

Verification of the Form 12 attached to the application for Import payments for customers X and Y showed that all the Form 12 supporting import payments were fake.

### **3.0 Typology 3: Abuse of foreign Currency**

The most recent typology that is appearing for the first time is on abuse of foreign currency access by some unscrupulous people. The FIA uncovered an emerging trend whereby some suspected black market foreign exchange operators disguised as Small and Medium Enterprises (SMEs) businesses abuse foreign currency facility by claiming foreign travel allowances using fake travel documents. The foreign currency accessed is sold on the unofficial market for a profit. Through analysis of suspicious transactions, the FIA established that bogus SMEs connive with travel agents who issue fake travel documents which are used to support claim of foreign currency. The suspicion is on the account transactions that involved deposit of huge amounts of money in the subjects' bank accounts that was immediately used to buy US dollars.

The SMEs open business accounts with financial institutions which are used to claim foreign travel allowances. The claims are disguised as genuine foreign travel allowance applications in which the procedures are followed as per Exchange Control Regulations. However, the travel documents (air-tickets and bus tickets) attached are fake. The purchases are not authentic and do not comply with Exchange Control Regulations.

## Case Study 3.1 Use fake travel documents to claim foreign travel allowance

### Case Study 3.1 Use fake travel documents to claim foreign travel allowance

The FIA conducted investigations in one Financial Institution Y by looking at about 400 beneficiary applications. The bus and air tickets which are proof that the applicant intends to travel were generally observed not to be genuine because they lacked characteristics of genuine tickets. There were several inconsistencies which are pointers to the likelihood of the tickets being fake as detailed below;

1. Different versions of tickets for Bus Company Q which often travels to Dar Es Salaam. The team discovered at least five versions of tickets issued by the company begging the question as to which ticket is genuine. The Bus Company Q also operates through appointed agents who issue the tickets on its behalf.

2. Travel dates; On the same bus tickets, it was also observed that some beneficiaries were in the Bank receiving travel allowance on the date that their ticket showed that they had already departed. For example on 18 July, 2016 Beneficiary R was at Financial Institution Y receiving foreign travel allowance while her Bus Company Q ticket showed that her date of travel was 17 July, 2016.

Similarly Beneficiary S had Air ticket number showing that her departure date was 17 July, 2016 but on 19 July, 2016 she was at Financial Institution Y receiving the travel allowance for the trip. This only supports the suspicion that the beneficiary did not actually travel to the destination.

3. Different beneficiaries using the same Air Ticket number; Some Air tickets bearing the same ticket number were being used by different applicants. On 19 July, 2016 two beneficiaries under Customer B attached the same Air ticket number. The expectation is that the Air-ticket number cannot be the same for two different individuals. It is highly likely that the Air tickets were fake and that the two beneficiaries did not travel to the indicated destination despite each applying and receiving US\$10,000 as foreign travel allowance. There was also repeated use of one Air-Ticket number from Airline C. These incidences point to the fact that people use fake travel documents just to meet the requirement of the regulations to obtain foreign travel allowance while in actual sense they do not travel.

4. Inconsistent information on Air-tickets; It was noted that most air tickets attached contained information which was inconsistent with information that is contained in a legitimate air ticket. Such inconsistencies include, the same Air ticket number having different issue dates for the going and return, incorrect flight numbers and departure times different from the real departure times of the flight number indicated.

5. Same ticket having two different names; ticket number PZ issued by Airline C to Passenger K of V Investment to Johannesburg, departing Blantyre on 5 June, 2016 and returning on 5 July, 2016 had different names for the passenger travelling to Johannesburg and another for the person travelling back. The return passenger was identified as Passenger W.

### **Case Study 3.2: Frequent use of one Travel Agent**

#### Case Study 3.2: Frequent use of one Travel Agent

It was also noted that about 90 percent of the air tickets attached are indicated as being issued by H Travel located at Z COURT in Blantyre. The Air-Tickets had one contact person indicated with a single mobile phone. There was no ground line. When Financial Institution Y called the contact person to confirm authenticity of the tickets, the contact person confirmed all the tickets as genuine. The contact person confirms when called that the air tickets were indeed issued by travel agent. It is highly likely that the contact person of the Travel Agent is part of the syndicate that fraudulently applies and receives foreign travel allowances.

### **Conclusion**

This report highlights financial crimes that occurred in the period 2015 – 2017. The methods include theft of pension funds by public officials, trade based money laundering and abuse of travel allowances. This report mainly targets the reporting entities to enable them to prepare for all kinds of eventualities and to be ready to detect and report suspicious transactions related to money laundering and financial crimes in general. In order to achieve this; reporting entities need to be well equipped by having adequate transaction monitoring systems and strictly adhering to KYC requirements and customer due diligence measures. Reporting entities need to be vigilant and properly identify their customers.