FINANCIAL INTELLIGENCE AUTHORITY

MONEY LAUNDERING TRENDS AND TYPOLOGIES REPORT

JULY 2020 - MARCH 2022

Building a Malawi free of financial crimes

Contents

PART A: GENERAL INFORMATION

FIA GENERAL INFORMATION

Registered name	:	Financial Intelligence Authority
Postal address	:	Private Bag B441, Capital City, Lilongwe, Malawi
Telephone number	:	+265 111 759 141
Website	:	https://www.fia.gov.mw/
Email	:	info@fia.gov.mw

ACRONYMS AND ABBREVIATIONS

Abbreviation	Definition
ATM	Auto-teller Machine
AML/CFT	Anti-Money Laundering/ Combating the Financing of Terrorism
DNFBP	Designated Non-Financial Businesses and Professions
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FCA	Financial Crimes Act
FIA	Financial Intelligence Authority
KYC	Know Your Customer
LEA	Law Enforcement Agency
ML	Money Laundering
MVTS	Money and Value Transfer Services
NPM	New Payment Methods
NPO/NGO	Non-Profit Organisation/ Non-Governmental Organisation
POS	Point of Sale
STR	Suspicious Transaction Report
TF	Terrorist Financing

1. INTRODUCTION

1. Section 4 (d) of the Financial Crimes Act, 2017 provides for the Financial Intelligence Authority (FIA) to conduct research into trends, techniques and developments in the area of financial crimes including Money Laundering (ML). Anti- Money Laundering (AML) and Combating of Financing of Terrorism (AML/CFT) work involves tracing and confiscation of proceeds of crime and Terrorist Financing (TF). This is done to improve the detection, prevention, deterrence and futility of Money Laundering (ML), Terrorism Financing (TF) and other financial crimes. The Trends and Typologies Report is developed based on the observations and analysis of tendencies, styles annotated and obtained from information received from reporting entities under AML/CFT regime in the country. The report includes sanitised case studies, which are just a fraction of the work done by the FIA in the period under review.

2. The Trends and Typologies Report can be used by the stakeholders in the fight against financial crimes. These include financial institutions, competent authorities, international counterparts and the general public. It is full of intelligence which enriches the stakeholders with good proactive and reactive strategies in AML/CFT interventions. It is an essential source of knowledge on ML and TF and other financial crimes such as bribery, corruption and fraud. It also highlights the red flags reporting institutions should look out for when monitoring transactions. Although the cost of these crimes cannot be precisely measured, their effect is catastrophic. The effect of these crimes continues to be felt across the globe, thereby prompting governments to enhance combating efforts.

3. Besides reactive methods, world authorities are also adopting proactive means to fighting financial crimes. For this to be a success, access to

information is very critical. Relevant and timely access to information helps different agencies to adopt appropriate tools to inform their proactive strategies in fighting financial crimes. One way of having access to information is through technology. Technological advancements have made it possible to develop better and effective methods to enhance the fight against financial crimes. On the flip side, modern technological trends have also equipped criminals with new ways of committing financial crimes.

4. In addition, the Covid-19 pandemic brought a major shift in financial behaviours with both positive and negative consequences. For instance, there has been an increase in online purchases and use of New Payment Methods (NPM) due to wide spread lockdowns globally. This resulted in a rise in cases relating to illegal and irregular externalisation of forex. The situation was majorly driven by inadequate checks and balances during the Covid-19 pandemic era.

5. The FIA, therefore, believes that the strategic intelligence contained in this report will provide the relevant stakeholders with the necessary tools they need to develop proactive countering strategies to halt criminals and disrupt financial crime syndicates. Further, the FIA is confident that dissemination of the report will help to inform relevant institutions of the various financial crimes, their nature and extent. The FIA is hopeful that the information herein will help the stakeholders to develop appropriate proactive strategies needed in the fight against financial crimes. FIA believes that this report will consequently be one out of many contributing factors to the reduction of financial crimes, thereby, enhancing the integrity of the financial system in the country.

6. The discussion from sanitised cases contained in this report also serves as a deterrent to would-be criminals as they bring to the fore, FIA's work in tracing and confiscating ill-gotten funds.

2. EXECUTIVE SUMMARY

7. As the Principal National Agency responsible for preventing and combating financial crimes, the FIA realises the important role that financial crime trend analysis plays in equipping stakeholders in the AML/CFT fight with strategic information. This information is critical to the development of effective proactive mitigating strategies in the fight against ML and TF by the various stakeholders that the FIA works with.

8. The FIA's 2021/2022 Trends and Typologies Report illustrates a range of trends observed in a number of areas. These include novel criminal tendencies such as the use of Non-Governmental Organisations (NGOs) to defraud people. The FIA has observed that fraudsters are preying on the public trust placed on NGO's to dupe people into depositing their funds with the NGOs. Such funds are disguised as registration fees for some promised benefits which range from agricultural farm inputs to education bursaries.

9. Other noteworthy new trends include layering of funds; dealings contrary to residential permit conditions; duping people into opening accounts or using third party accounts with an intention to use them for fraudulent activities.

10. The FIA has observed that criminals are increasingly layering funds through the financial system in order to distort the funds' criminal sources. Layering is a stage in the ML process through which criminal proceeds are distanced from their real sources. The process involves transferring of funds through multiple layers of transactions, usually of high value. Layering enables criminals to disguise illicit proceeds and move them through the financial system until they seem legitimate. These high value transactions are made

across several businesses and personal accounts and they usually do not make business sense.

11. In addition to these novel trends, the period under review has brought to light some common abuse of exchange control regulations. The global economy suffered some destabilizing shocks. This was partly due to the Covid-19 pandemic and other factors. This has compelled cross border traders in the country to devise illegimate ways of profiting from their money.

12. To this end, we have noted a new trend where cross border traders are accessing foreign currency through use of ATM cards. The traders prefer cashing at ATM machines outside Malawi. The practice is prone to abuse since some individuals are taking advantage of the situation and are selling back the foreign currency in border districts without satisfying licencing requirements. We have further noted that some individuals are abusing the facility by using ATM cards belonging to various individuals to cash foreign currency outside Malawi, and, in the process, violating some foreign currency exchange controls.

13. ML trends highlighted in the 2019-2020 Trends and Typologies Report have continued to manifest during the period under review. Some of these prominent continuing trends include ML from environmental crime; theft of public funds; trade-based ML, use of new payment methods; foreign currency exchange violations; use of false documents; financial institution fraud and under declaration of Know Your Customer (KYC) information.

14. It is worth mentioning that under-declaration of KYC information has led to some reported Suspicious Transaction Reports (STRs) not being analysed further for lack of adequate client information provided at the time of

opening accounts. The FIA has further noted that in the past, fraud within financial institutions was perpetuated through bank employees transferring funds from suspense accounts to their own or other people's accounts. The new *modus operandi* is one where bank employees commonly understate cash deposits made into less active accounts and then profit from the difference. Mostly targeted are dormant accounts or accounts of Malawians living outside the country. The low activity in such accounts renders detection of the diverted funds almost improbable and, if, there is ever suspicion, it usually happens after a lot of funds have already been diverted to the bank employees' account/s.

15. The FIA also noted an emerging and frequently appearing fraud in form of tax evasion. It manifests through individuals trying to conceal their business' taxable income in order to pay less taxes. This is achieved through under-declaration of revenue, non-payment of customs duty or mis-declaration of products in order to pay less duty.

PART B: OVERVIEW OF STRs RECEIVED

3.General observations from STRs and Financial Investigations

16. This section outlines an overview of the STRs that the FIA received from reporting entities and consequently analysed. Reporting entities are obliged by law or regulations to report promptly their suspicions to Financial Intelligence Units (FIUs) if they suspect or have reasonable grounds to suspect that particular funds are the proceeds of criminal activity, or are related to TF.[1]

[1] www.fatf-gafi.org

17. The section also gives a snapshot of the information shared by FIUs in other countries on suspicious activities they have observed in their jurisdictions relating to financial crimes connected to Malawi. It further details some of the financial investigations that were conducted and the financial intelligence disseminated to Law Enforcement Agencies (LEAs) and other relevant stakeholders.

18. STRs are an important source of information as they may lead to the identification of predicate offences resulting from ML, TF and Proliferation Financing (PF). The information is later analysed and disseminated to relevant LEAs and, through this analysis, illegal sources of funds may be identified. Also, patterns and trends of criminal activity may be uncovered. Additionally, vulnerabilities and indicators of ML/TF techniques and methods are also identified.

19. As was pointed out in the introduction to this report, it is important to note that these indicators will significantly support the reporting institutions under the AML/CFT regime in monitoring transactions and in developing efficient and effective AML/CFT policies. An efficient AML/CFT regime is imperative for preventing individuals and criminal organizations from using a financial system to launder proceeds derived from illegal activities. In the end, the integrity of the financial system is maintained. Moreover, the identified indicators will help LEAs in developing effective investigative techniques to combat ML/TF and other financial crimes. For the general public, the report is an essential awareness tool on the methods that criminals use to deceive and defraud them or dupe them into being used as innocent accomplices.

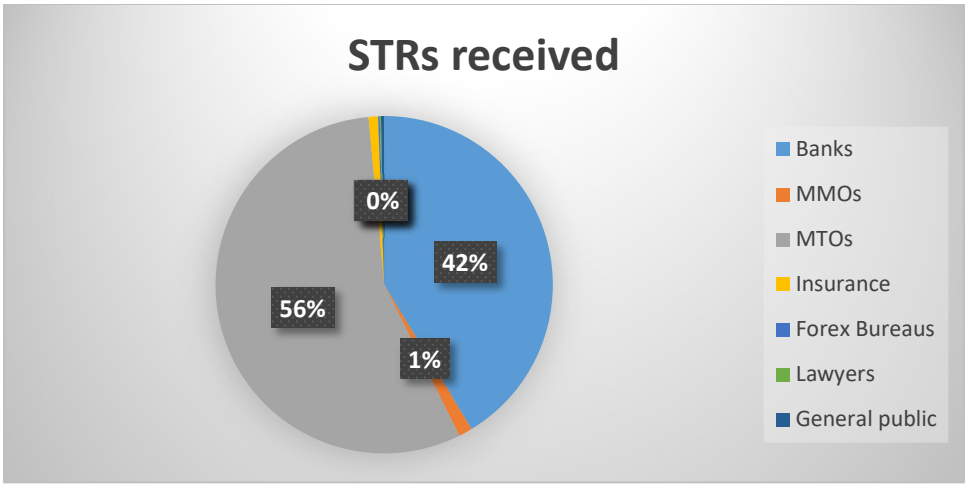
- Information that has been used to produce this report has been derived from the following sources;STRs that were received and analysed from various reporting entities under AML/CFT for the period between July

2020 and March 2022. The STRs were filed with the FIA by banks and Designated Non-Financial Businesses and Professions (DNFBPs). The total number of STRs received was **675,** of which **279** were from banks**,** representing **41%, 377** received from Money Transfer Operators, representing **56%.** The remaining **25** STRs were received from; Insurance Sector, Mobile Money Operators (MMOs), Foreign Exchange Bureaus, Lawyers and the general public, representing **3%.** The FIA did not receive any STR from some segments of reporting DNFBPs such as the Real Estate sector, Dealers in Precious Stones and Metals, Accountants and Casinos.

- Requests for information from LEAs
- Media reports and other open sources
- Publicly available information
- Previous trends and typologies reports
- Sanitised cases from LEAs.
- Information provided by other FIUs.

20. Pie chart 1 below presents summary statistics of STRs received by FIA from the reporting institutions by sector. Notably, the Financial Institutions sector is leading in the reporting of STRs compared to other sectors.

Pie chart 1: STRs received from reporting sectors



4. Common indicators observed

Below are some of the most prevalent techniques, indicators and red flags that triggered and raised suspicion on possible financial crimes, ML, TF and other financial irregularities.

- Business accounts receiving huge amount of funds transfers inconsistent with the business profiles. In addition, personal accounts are used for business purposes.
- Cash deposits followed by immediate cash withdrawals of equivalent amount. Usually, the deposits were made by different individuals in different locations. In other instances, the deposits were made from one specific geographical location. The transactions do not make business sense when compared to the KYC information.
- Accounts being used as mules to transfer funds from third parties. This is common for import payments where business entities use agents to pay and transfer large amounts to foreign jurisdictions.
- Use of falsified documents to defraud accounts. Examples include; presentation of fraudulent cheques, using falsified documents in order to conceal the real beneficial ownership of a business, using falsified documents to obtain funds illicitly and using fake invoices for import payments.

- Misuse of New Payment Methods such as virtual cards and mobile payments. Individuals opening and/or having access to multiple accounts and cards through which they transact to the maximum limit permissible.
- Misuse of Money Value Transfer Services (MVTS) seen through the use of multiple persons to send money to people in other jurisdictions. There are no apparent links and affiliation between sender and receiver.
- Tax evasion through structuring of import payments so that each importation is below the limit for customs duty. This is done when a businessperson imports a large consignment of goods but which were paid for and received as multiple small parcels.
- Unreconciled returns following import payments. There is a trend where customers apply for additional international remittance of funds before they reconcile previous payments. Some customers jump from one bank to another yet they have unreconciled returns.
- Concentration of transactions in the border districts. Threats and vulnerabilities have been identified which are emanating from the high concentration of cash flowing towards the border districts of Karonga and Mchinji which border Tanzania and Zambia respectively.
- Multiple third-party cash deposits into the same account followed by outward international transfers.
- Fraudsters deceive their victims into disclosing confidential information thereby hacking the victims' accounts. Similarly, fraudsters trick unsuspecting people into giving information over the internet or by email in order to defraud them of their money.
- Impersonation of LEA officers by fraudsters. On a number of occasions, fraudsters have attempted to defraud individuals by posing as officials from LEAs. In some cases, the victims were tricked into believing that a particular LEA had frozen or confiscated funds sent to them from abroad and that they needed to pay some kickbacks for the funds to be released.

- Employees of Financial Institutions conniving with fraudsters to falsely register customers on mobile payment platforms.
- Ponzi investment schemes. People are being tricked to make contributions towards high yielding investment portfolios. They are advised to recruit others for better returns. Victims willingly and blindly join the schemes.

5. MONEY LAUNDERING METHODS AND TRENDS 2020-2022

21. The FIA reviewed and analysed the STRs and requests received during the period 2020/2022, and has observed several emerging and on-going ML methods and techniques. In particular, the FIA notes the use of electronic and new payment methods emerging as a major threat and enabler of ML activities in the country. Of interest is the use of ATM cards, electronic purses, mobile payments, online and internet payment services.

22. Technological advancements and the dynamic nature of these methods has created opportunities for criminal syndicates to exploit the systems as a conduit for ML activities. This trend is not at all surprising as use of these

methods is common in the global economy. The Covid-19 pandermic further accelerated use of digital and modern payment methods.

23. In Malawi, common trends that have been noted include cases of moving illicit funds across borders. In such cases, the perpetrators use ATM Cards to withdraw huge sums of money across borders and use online payments to transfer money between businesses to avoid detection. A number of people have been arrested in neighbouring countries possessing multiple visa cards belonging to numerous persons, which they were using for cash withdrawals.

24. In addition, environmental crimes continued to pose a threat to Malawi's flora and fauna. The major species heavily threatened in Malawi are elephants, hunted for their ivory and pangolins for their scales and meat. There have been investigations and prosecutions of illegal wildlife trade kingpins leading to their convictions. Pangolins have become the most trafficked wildlife in Malawi.

25. The FIA continued to see cases of Trade Based Money Laundering (TBML). This is the movement of illicit proceeds through the exploitation of trade transactions. TBML remains a major threat to Malawi since the final destination of the funds is usually unknown.

26. TBML is becoming more complex because foreign nationals are recruiting Malawians to register businesses or companies and make import payments for goods which never come to Malawi. They also make huge payments for low value goods just for the purpose of moving funds.

General overview of ML methods and trends

i. Use of New Payment methods to move and access illicit proceeds.

- Criminal syndicates use online payment systems, mobile payments, electronic purse and prepaid cards to move funds across the borders and make withdrawals.
- Boarding customers on mobile platforms without their knowledge in order to get access to multiple visa cards for use across the borders.

ii. Use of legal entities as fronts to launder proceeds of crime such as;

- Wildlife syndicates using a shell company to obscure proceeds of crime and beneficial owners.
- Foreign nationals using legitimate businesses as a front for illegal wildlife trade.
- Wildlife crime syndicates involved in illegal loan shark businesses to launder proceeds.

iii. Corrupt public officials often using third parties to receive and transfer the illegal proceeds and to conceal properties obtained from proceeds of crime. Examples of the illegal sources of such illegal proceeds include the following;

- Public officials acquiring and possessing unexplained wealth.
- Involvement of public officials in procurement fraud, abuse of office and money laundering.
- Abuse of funds meant for Covid-19 response by public officials.

iv. Collusion between employees of reporting entities and crime syndicates to circumvent transactions requirements.

- Processing import payments without making enhanced customer due diligence of the sender and beneficiaries.
- Bank officials processing import payments by ignoring Exchange Control Regulations i.e. allowing import payments without supporting documents.

- TBML is a growing concern in the banking sector with the growth in international trade. The major drivers have been collusion between importers and exporters and inducements given to bank officials to carry out illegal transactions. Concealing information about the beneficial ownership or control of funds. This happens mostly to hide the link between the source of funds and a criminal act.

- Creating an impression that the transaction is legitimate where it may raise suspicion, if correct information is provided.
- Use of fake business registration certificates, fake identities and fake import documents.
- Companies making false declarations to evade tax.

v. Businesses and traders involved in Exchange Control Act violations

- Traders making ATM cash withdrawals in foreign countries using multiple VISA debit cards belonging to self and third parties
- Traders using bank accounts to engage in illegal externalisation of funds.

vi. Fraud by employees of reporting entities

- Bank employees understating cash deposits by customers.
- Bank employees abusing online payment systems.
- Bank employees swindling cash recovered from fraud cases.

vii. Creating and using false documents to fulfil KYC requirements

- Perpetrators using false documents to open bank accounts with the aim of committing fraud.
- Perpetrators using falsified documents to conceal business ownership when registering companies. The companies' bank accounts were later used to embezzle public funds.

viii. Providing false information to meet customer identification requirements

- Failure to update KYC information in order to circumvent transaction requirements.
- Failure to properly register Non Profit Organisations (NPOs) to defraud people and launder funds.

PART C: MONEY LAUNDERING, TERRORIST FINANCING TRENDS AND TYPOLOGIES

6. CONTINUING TRENDS

6.1 Typology 1: Theft of public funds

Introduction

27. During the period under review, the FIA noted a trend on an on-going basis of abuse and theft of public funds, particularly under Other Recurrent Transactions (ORT). Due to payment system failures, some powerful public officials withdrew huge cash amounts from Government accounts, thereby engaging in third party ML. Third parties were used to blur the connections between public officials, the laundering process and the proceeds of their crimes. This is called third party money laundering.

28. The withdrawals were made under the disguise of internal and external travel allowances without any supporting documents containing details of the individuals undertaking those trips. For instance, there was a Malawi Government vote in which over MK2 Billion was withdrawn in just under six months. The records show that two officers were everyday making cash withdrawals from the bank. Thereafter, third parties would then deposit funds into the bank accounts of the concerned public officials. Part of the funds were used to buy assets through third parties. Findings of the preliminary concealed income analysis showed that the public officers had accumulated unexplained wealth.
29. Some cases handled recently by the FIA also showed a major money laundering trend in which public officials used loans to layer and integrate proceeds of crime into assets such as real estate and motor vehicles. The officials laundered the funds by obtaining loans which were repaid using cash payments or smaller structured cash amounts. Some loans were repaid in full before realisation of the agreed repayment period. It is highly likely that the loans were essentially taken out as a cover for laundering proceeds obtained through theft of public funds under the guise of repayments. Transactions related to a loan may attract less scrutiny than significant cash activity.
30. In the period under review, Malawi also experienced Covid-19 related money laundering. Covid-19 funds were abused through procurement processes. Some public officials misused the processes for procurements under emergencies as was the case with Covid-19 related procurements and the lack of adequate scrutiny of the resulting payments. This was unveiled after a forensic audit. 6.1.1 Case Study 1: Public officer arrested for possession of unexplained wealth

Case Summary

Offence	Theft by public officer

Customer	Individual/business
Products and services	Cheques, bank accounts and loans
Indicators	• The transaction was inconsistent with the customer's profile • High volumes of transactions within a short period of time • Large cash deposits used for investments • Large amounts of cash from an unexplained source • Multiple loans obtained over a short period of time with early repayments made in cash

Case Description

The FIA is part of an inter-agency task force that arrested a suspect working in the public service for suspected money laundering offences. FIA analysis established that the suspect had an unknown/illegal income of over MK2 Billion. The assets in form of real estate, motor vehicles and funds of over MK100 Million in various bank accounts are under preservation.

FIA established that the suspect siphoned millions of cash from public institutions through unsupported cash withdrawals, claims for internal and external travel allowances and government cheques paid to his business for unknown services. The suspect laundered the funds through the purchase of real estates, motor vehicles and investment into various businesses. The suspect accumulated wealth not commensurate with his known sources of income.

The suspect used loans to layer and integrate illicit funds stolen from Government into real estates. The suspect then laundered the funds by obtaining huge loans in succession from one of the financial institutions which he was repaying through

lump-sum cash payments and structured cash amounts originating from stolen government funds. One loan of over MK300 Million was repaid within six months. The loans were essentially taken out as a cover for laundering criminal proceeds under the guise of repayments. Transactions related to a loan may attract less scrutiny than significant cash activity.

FIA established that over a period of about five years, the suspect's income from legal and known sources amounted to about MK800 Million. The known expenditures during the same period amounted to about MK3 Billion. The difference between income from the legal or known sources and the known expenditures was over MK2 Billion. The difference is enormous and may not be reasonably explained for a public servant.

Subsequent action

Arrests

Asset recovery processes

6.1.2 Case study 2: Public official arrested for procurement, abuse of office and money laundering

Case Summary

Offence	Money laundering, abuse of office
Customer	Company/individual
Products and services	Cheques, bank accounts and loans
Indicators	• Cheques paid to companies owned by associates • Associates with multiple accounts under multiple names • Using fake identification • The transaction was inconsistent with the customer's profile

	• High volumes of transactions within a short period

Case description

FIA assisted law enforcement agencies with an investigation which led to the arrest of a former public official together with one business person for being suspected of procurement fraud, abuse of office and money laundering. The suspects are being prosecuted. In addition, the tainted property was restrained.

The FIA established that the former public official and the business person registered two companies (Company V and D). In both companies, the two are shareholders. Company V was awarded a contract to supply goods by a public company where the public official was one of the Directors. The funds involved were estimated at MK150 Million. The law enforcement agencies established that the contract was fraudulently awarded by the former public official. It was further established that the public company made unusual cheque payments to Company V. The cheques paid to Financial Institution N, were accompanied with instructions to pay Company V with funds in accounts held in Financial Institution C.

FIA established that a bank account for Company V was opened as a front business to introduce illicit money into the financial system. The illicit money was obtained through procurement fraud before it was transferred to personal bank accounts of both suspects. The suspects targeted one financial institution's account opening procedures to build false customer profiles which they used to present Company V as a legitimate business. Further, the public official presented a fake identification document when opening the business account to hide beneficial ownership of the funds.

Subsequent action
Investigations
Arrests
Prosecution
Seizures and restraining orders

6.1.3 Case study 3: Public officials arrested for abuse of Covid-19 funds

Case Summary

Offence	Theft of public funds
Customer	Individual, business
Product and services	Cheques, bank accounts and loans
Indicators	• The transaction was inconsistent with the customer's profile • High volumes of transactions within a short period of time

Case description

In one procurement case, a Government institution handpicked a contractor to provide some services to mitigate the impact of the Covid-19 pandemic. The contract was worth MK100 Million. The services could have alternatively been provided at a lower cost by officials from the Ministry of Health but the Government Agency instead engaged a private entity, thereby causing the Government to spend more on the service. A service which Ministry of Health required MK2 Million to implement, the private contractor instead demanded

MK30 Million. A relevant law enforcement agency arrested the contractor and one public officer from the Government institution that awarded the contract. The two are being prosecuted. Funds amounting to MK20 Million were frozen.

In a related case, a government department used funds that were meant for Covid 19 pandemic interventions to pay for the ORT for institutions. Following the discovery of the misprocurement and mispayment, the agency was made to refund the COVID funds and officials from the agency were disciplined, while somewere dismissed from employment.

Subsequent action

Freezing account

Investigation

6.2 Typology 2: Money Laundering from Environmental crime

Introduction

31. A law enforcement task force conducted an investigation relating to a wildlife trafficking syndicate in Malawi. Sixteen syndicate members (Twelve foreign nationals and 4 Malawians) were arrested. The suspects were charged with various offences ranging from possession and dealing in wildlife trophies to money laundering. Fourteen syndicate members were convicted and sentenced to various years ranging from 1 to 14 years imprisonment.

32. The investigations unearthed the syndicate's money laundering schemes in the banking system and the casinos. The syndicate used banks and casinos to introduce their illicit proceeds from wildlife products, into the formal financial sector before transferring and investing into the real estate sector.
33. Another lucrative illegal wildlife trade in Malawi is trafficking of pangolins. In 2020 and 2021, LEAs handled 75 cases, made 133 arrests and seized 89 Pangolins. Most of the arrests were made at the time when the traffickers were selling the animals. The price ranged from MK2 Million to MK10 Million although in some cases, the price was as low as MK800, 000.

6.2.1 Case Study 1: Wildlife syndicate using a shell company to hide proceeds of crime and beneficial owners

Cases Summary

Offence	Money laundering
Customer	Company/individual
Product and services	Cheques, bank accounts and loans
Channel	Cheques, Electronic transfers
Indicators	• Account activity inconsistent with customer profile • Multiple electronic transfers from third parties • Multiple cash depositors linked to the same address • Cash deposits followed by immediate withdrawals • Account signatory unaware of most of the transactions

Case description

From 2019, the FIA conducted parallel financial investigations on high profile illegal wildlife trade cases. The results were disseminated to LEAs and eventually this led to the arrest of 2 foreign nationals. The prosecution of the 2 suspects is ongoing. Furthermore, a preservation order was obtained on the assets.

FIA established that Foreign National A laundered proceeds of crime through a shell company which was properly registered with the Registrar of Companies. He opened two bank accounts with one of the banks in Malawi. The suspect exploited Know Your Customer (KYC) procedures to present a shell company as a legitimate business in Malawi. The suspect was a dependent and was in Malawi under the parents' resident permit. The suspect did not have the financial muscle to run a company. The parents used the suspect to conceal the origin and ownership of the funds.

The shell company received over MK400 Million from various sources in forms of transfers, cash and cheque deposits. The depositors were purportedly paying back funds they had borrowed from the suspect and her husband. The suspect and her husband operated a loan shark under illegal conditions contrary to the declared source of income at the time of opening the account. The two had declared funds will come from the purpoted business of manufacturing and sell of ironsheets.

The suspect's mother, father and husband were arrested and charged with wildlife offences. They were all convicted and are currently in prison. The investigations pointed to a connection between the funds that were being deposited and the wildlife specimen. The source of funds used in loaning out to individuals whose repayments ended up in the shell company account may have been partly from the trade in wildlife specimen. The funds were laundered through a loan shark business and later ended up in the shell company to make them appear legitimate.

Subsequent Action

Investigations Arrests Preservations Prosecution

6.2.2 Case Study 2: Arrests for being found in possession of Pangolin

Case summary

Offence	Possession of protected species, Money laundering
Customer	Business and individual
Product and services	Cheques, bank accounts and loans
Channel	Cheques, cash deposits
Indicators	• Account activity inconsistent with customer profile • Business address linked to the same address as syndicate members • Cash deposits followed by immediate withdrawals • Account signatory is out of touch with most of the transactions

Case description

FIA shared financial intelligence with LEA on two traffickers who were found in possession and smuggling of a pangolin. The two were part of the largest wildlife trafficking syndicate in Malawi. One of the traffickers registered a business and

opened a bank account with one of the major banks in Malawi. He declared that he was a sole trader in a wholesale business. His source of capital was borrowed funds.

The physical location of the business was indicated as a plot owned by another foreign national who was part of the illegal wildlife crime syndicate. He received funds in his account followed by immediate withdrawals. The trafficker also received MK5 Million cheque payment from the business account registered in the name of a third foreign national, who is also a member of the syndicate.

It is suspected that the trafficker operated as a money mule paid by the foreign nationals who run the syndicate. He was being used by the syndicate to make payments for the pangolins, other trafficked wild animals and specimen. This way, the syndicate transacted without being linked to the crime. The two traffickers were convicted and sentenced to 3 years imprisonment.

Subsequent Action

Arrests

6.3 Typology 3: Trade-Based Money Laundering

Introduction

34. Trade Based Money Laundering (TBML) continues to be a significant money laundering risk in Malawi based on the reports from the Financial Sector and analysis by the FIA. It is a great risk considering the amount of tax revenue loss and the loss of economic integrity the country faces. TBML seems to go unnoticed because of the seemingly victimless nature of the crime.
35. Some employees of the Financial Institutions play a part by accepting requests to handle the transactions and move the funds even when they know that the request is bogus. The requests are not scrutinized and often, the transactions take place away from where the bank account of the trade entities are domiciled.
36. More often than not, reporting is done after huge volumes of funds have already been moved. In particular, when bank employees are discovered to have facilitated transactions whose documentation is irregular, they just resign. The employees seem to corruptly facilitate TBML.
37. The characteristics of TBML in Malawi are as follows;

- Unreasonable requests for advance payments for shipments.
- Inability to produce appropriate documents (invoices) to support a requested transaction.
- Significant discrepancies between the description of goods on the transport documents and the invoices.
- Trade entity suddenly closing bank account with one financial institution after transferring huge amount of funds and opening another bank account with another financial institution.
- Trade entities ordering goods from suppliers in a different line of business from their stated business.
- Trade entities making late changes to beneficiary supplier details without reasonable explanation.

- Trade entities willing to incur significant charges in the process of conducting transactions.
- Importing and making remittances for non-essential goods.
- Over and under-invoicing.

6.3.1 Case Study 1: Trade-Based Money Laundering through phantom shipments

Case Summary

Offence	Money laundering
Customer	Business/individual
Product and services	Cheques, bank accounts and bank transfers.
Channel	Remittance
Indicators	• Account activity inconsistent with customer profile. • Frequent cash deposits immediately followed by request for foreign advance payments. • New account making frequent remittances • Foreign suppliers' line of business different from goods indicated on the invoice.

Case description

FIA analysed and disseminated to law enforcement a report of a suspected trade entity which remitted over MK300 Million in two months. The funds were remitted as foreign advance payments made through two financial institutions.

A particular LEA conducted investigations into the trade entity's remittances. The trade entity had just registered the business and opened accounts in financial institutions. The registered owner was unable to explain the source of funds. He later confessed to being used by some foreign nationals to facilitate the transfer

of funds through bogus trade transactions. It is unusual for a recently opened business to make remittances in large amounts.

Analysis showed that the account of the trade entity received frequent cash deposits, and these were followed by outward remittances made in form of advance payments for irrigation equipment. Almost all cash deposits were made by the registered owner of the entity. Within 3 months, the trade entity remitted about MK300 Million to various suppliers in one foreign jurisdiction. The destination and type of commodities being imported were inconsistent with the known business type of the beneficiary/supplier. The invoices were for irrigation, solar and electrical equipment yet, the suppliers involved were engaged in food industry.

The outward remittance transactions by the trade entity were repetitive and frequent, hence, did not make any economic sense. The financial institutions did not follow the KYC procedure to the letter, thus, to visit and verify the physical premises of the business entity. The invoices from the two suppliers appeared to have the same font type, size and design indicating a likelihood that the invoices were from the same source. In addition, there were no payments to Malawi Revenue Authority (MRA) for import duty by the trade entity. The registered owner of the trade entity confessed that no goods would be shipped to Malawi despite funds being remitted under the pretext of ordering irrigation equipment. Thereafter, the trade entity account became dormant.

The LEA arrested the registered owner of the trade entity and prosecution is still in progress.

Subsequent action

Prosecution is still ongoing.

6.3.2 Case Study 2: Abuse of the International Trade system in Malawi

Case summary

Offence	Money laundering
Customer	Business/individual
Product and services	Cheques, bank accounts and bank transfers
Channel	Remittance and international trade
Indicators	• Frequent cash deposits immediately followed by request for foreign advance payments • Trader maintaining multiple accounts • Frequent request for import payments across multiple accounts for same goods by same supplier • Frequent receipt of cash deposits from third parties • Willingness to face high import payment charges, no concern for possible business loss • Willingness to accept higher foreign exchange rates and currencies that do not make business sense.

Case description

FIA analysed a report of a suspected sole trader who remitted over MK17 Billion in just under two years through two financial institutions by using four bank accounts. The beneficiaries of the funds are entities located in neighbouring countries to Malawi. The sole trader deals in wholesale business selling mainly inexpensive grocery items such as sweets, chewing gums, low-priced chocolates, dry yeast, laundry soap, football cup stickers, toilet paper and other trivial items. The sole trader operates under 2 business names and owns one small shop. The transaction pattern shows that the trader could be part of a money laundering syndicate involved in moving large amounts of money internationally under the guise of trade. The results of analysis showed the following;

-Possible falsification of invoices as observed in sudden fluctuation in invoice amounts from the same foreign suppliers for the same goods and quantity.

-More than 350 import payment transactions involving 2 banks in just under 2 years for inexpensive goods.

-Unnecessary exertion of pressure on banks to conduct transactions even if the trader would incur high charges.

-Simultaneous request for import payments by the sole trader in the two banks for similar goods.

-The sole trader was always on priority list of customers to be considered for import payments by the bank even in instances of lean foreign currency availability and even though the goods being imported were available locally and were not priority goods.

-The import payments were repetitive and did not make economic sense.

-Frequent receipt of cash deposits from third parties followed up by request for import payment.

Subsequent action

Investigations

Prosecution

6.4 Typology 4: Foreign Currency Exchange Control violations

Introduction

38. The increase in access to electronic banking, such as Electronic Fund Transfers (EFTs) and the use of debit cards among others, has substantially eased banking processes in light of the Covid-19 pandemic. Despite this being a positive development, some individuals also are abusing the system by illegally externalising foreign currency through such means as

ATM withdrawals. According to Exchange Control Regulation 10 sub-regulation 1, any person, other than the bank or an unauthorized dealer, who sells foreign currency to anyone is liable to an offence, fine or imprisonment.

39. The FIA has observed a common trend where some bank customers regularly deposit large amounts of money in cash or EFTs into their accounts, then later access the funds in foreign currency through Merchant Point of Sale (POS) and ATMs in other jurisdictions. These people then bring back home the foreign currency to sell on the black market and at the borders.

Case summary

Offences	Operating a Financial Institution without Licence
Customer	Individual
Products & services	Bank accounts, ATM cards, cash
Channels	ATMs, POS devices, travel allowance. Informal (black) markets
Indicator	• Frequent Large deposits into a bank account followed by withdrawal of same amount across the border through ATM. • Frequent application of travel allowances. • Different bank accounts being credited by one source. • Possession of several ATM cards of other people.

Case Study 1

Several customers holding accounts with various financial institutions were caught with multiple debit cards while withdrawing funds outside Malawi. Frequent large cash deposits were made into various banks accounts belonging to them and

other third parties. Arrests were made in a number of Jurisdictions including; Kenya, Zambia, Tanzania and United Arab Emirates (UAE). Some of the culprits were repatriated to Malawi and are answering various charges.

The emerging trend shows that some perpetrators approach other individuals to open bank accounts and then get custody of theirATM cards to use them for forex externalisation. In one incident, the FIA analysed and investigated a case in which the perpetrators registered a security company and took a group of people to open bank accounts through an agent. The people were disguised as employees of the security company. Later, the agent collected the ATM cards and gave them to the business men. The businessmen credited the accounts of the alleged employees. The funds were later withdrawn from the ATM in foreign jurisdictions. The culprits were arrested while trying to withdraw the funds and had 40 ATM cards in their possession.

Subsequent Action

Arrests

Freezing of bank accounts

Preservation of funds

6.5 Typology 5: Irregular forex externalisation through abuse of debit cards.

Introduction

40. While our investigations and analysis show that it is common for cross-border traders to carry plastic money and access the funds from ATMs as foreign currency in bordering countries, we have also observed that even non-crossborder traders are engaging in the same practice to benefit from competitive rates of other foreign currencies over the Malawi Kwacha.

41. The practice is becoming a conduit for illegal forex externalization and terrorist financing (TF) since not everyone accessing foreign currency in the bordering countries is doing so for cross-border trading purposes. Again, the individuals selling the foreign currency at the borders violate the exchange controls in place because they sell the foreign currency without authorization. Observations and findings from analysis and investigations on some of the transactions established the following;

    - There are a lot of micro and small business enterprises which are importing merchandise from the neighbouring border districts. To minimize the risk of carrying cash over a long distance, the business persons are using ATM cards as 'cash couriers' to carry their cash from one point to another.

      The Covid-19 pandemic has introduced a new way of doing business where middlemen are used to purchase goods across the borders and send them to the clients in the mainland. Most of these middlemen operate along the border districts. Therefore, funds are deposited from other locations to the middlemen in the border districts.
    - Third parties open accounts on behalf of others with full knowledge of aiding the externalization of funds.
    - Bank customers being deceived to open and/or share debit cards which were used for withdrawing foreign currencies.
    - Source of the externalised funds is usually unknown and maybe proceeds of crime.
    - The money accessed through cross-border ATMs is more than what can be disbursed from an ATM in Malawi.

42. FIA analysis has identified the following enabling factors that promote and encourage the foreign currency control malpractice and abuse of debit cards:

- Limitations on travel allowances;
- Scarcity of forex in the financial institutions;
- Challenges to access forex timely;
- Reluctance by some traders in neighbouring countries to accept Malawian currency for trading in the border districts.

43. For illegal externalisation of foreign currency, it was noted that few people who open the accounts on behalf of others do so with full knowledge of what will happen while most people are duped. The account holders are promised jobs, loans for businesses, and sometimes given monetary incentives.

6.5.1 Case Study 1: Unusual withdraw of funds from border districts and countries

Case Summary

Offences	Illegal externalisation of forex, money laundering
Customer	Individual
Products & services	Bank accounts, ATM cards, cash
Channels	ATMs, POS devices
Indicator	• Frequent large deposits into bank aaccounts followed by withdrawal of same amount at border district or country through ATM. • Third parties exercising control and ownership of a bank account is different from the one who opened it. • Different bank accounts being credited by one source. • Possession of several ATM cards of other people.

Case Study 1

Several customers holding accounts with various banks were found to be abusing the debit card facility. Large cash deposits were made into their accounts and withdrawn through ATMs and POS machines in bordering countries. FIA received more than 60 STRs in relation to such transactions from one reporting entity. The emerging trend is where some unscrupolous business people approach other people to open bank accounts on their behalf for the purpose of obtaining ATM cards to be used for forex externalisation.

Results of investigation and analysis of the reports revealed that once bank accounts are opened, the business people have total control of the bank accounts. For example, they deposit and withdraw funds, get hold of the ATM cards from the purported account holders. The account holders also provide their contact details, for example phone numbers, for mobile banking platforms.

Subsequent action

Investigations

Frozen bank accounts

6.5.2 Case Study 2: Using bank accounts and ATM cards of third parties to conduct illegal externalisation of funds

Case Study 2: Using third parties to open bank accounts

In 2021, Mr. X was approached by Mr. Y to open a bank account at one of the branches of Bank A. Mr. Y alleged that he had lost his national identity card, as such, he could not access funds from people who were to send him money. Together, they went to the Bank to fill out account opening forms. However, Mr. Y insisted that for phone contacts, a different number (not belonging to either of them) be indicated on the form. This raised suspicions and prompted Mr. X to report the matter to the Police.

Preliminary investigations by the Police established that Mr. Y was an agent, acting on behalf of Ms. Z. It transpired that Mr. Y had by then already recruited several unsuspecting customers and enticed them to open bank accounts. The ATM cards were subsequently collected by Mr Y and taken to Ms. Z. She used to deposit large sums of cash into the accounts and later withdraw the funds in foreign currency.

Subsequent Action

Arrests

Prosecution

Case Study 3: A lady arrested for being found with more than 40 ATM cards

Following an STR from Bank Y, the FIA analysed and investigated a case where Ms. X was arrested by the Police for being found in possession of more than 40 ATM cards of Bank Y belonging to different people. Ms. X visited her home village where she told a group of women that she runs a microfinance organisation that provides loans.

She convinced the women to open bank accounts which they could be using to access loans from her alleged microfinance organisation. She provided the funds for the opening of accounts and ATM cards. When the accounts were opened, she collected ATM cards from the women. Following this, Ms. X started transferring funds to the accounts which she subsequently withdrew from ATMs in a neighbouring country to buy merchandise for resale in Malawi.

Subsequent Action

Reported to RBM

Investigations

6.6 Typology 6: Use of New Payment Methods (NPM) and alternative methods.

Introduction

44. New Payment Methods are inventions that use the Internet, wireless devices, and payment networks for purposes of remitting and receiving funds globally. These include; Mobile money platforms, virtual cards, prepaid, and online payments services.

45. There has been continued use of Money or Value Transfer Services (MVTS) facility to illegally remit funds internationally. MVTS providers are vulnerable to abuse of money laundering and terrorist financing. Among these, is the unusual externalization of funds through XZY Agency; a well-known international MVTS. Some commercial banks have opened up the XZY Agency facility, where customers receive from and remit to other countries using the facility.

46. A worrisome trend has been noted on the misuse of this facility. Individuals of Malawian origin have opened bank accounts and used these bank accounts to receive money from foreign nationals within Malawi. Immediately after receipt, the funds are externalised to countries of the foreign nationals using the XZY facility.

47. Furthermore, FIA has observed that huge amounts of money are being remitted within a short period of time. In addition, the payment narrations do not reflect the purpose of transfers being made. Further, the individuals involved lack awareness on the implications of sending money to high-risk countries.

6.6.1 Case Study 1: Structuring funds for cross-border wire transfers

Case summary

Offences	Money laundering, illegal externalisation of foreign currency
Customer	Individuals
Products & services	Cash, bank accounts
Channel	Remittance Services, MVTS
Indicators	• Amounts being credited to the account not corresponding to the declared amount. • Multiple third-party cash deposits into the same account followed by outward international transfers to multiple individuals. • The frequency of deposits not making sense. • Narrations on the transfers made not reflecting the declared purpose of transactions. • The source of funds on KYC declarations different from the purported reason for payments.

Case description

The FIA analysed a report on a Malawian customer, Mr. A, who opened an account with Bank X. When opening the account, Mr. A declared MK 300,000.00 as his monthly income. After an estimated three months, Mr. A's account was credited with more than MK60 Million. Out of this, MK58 Million was remitted to Country Y, an Asian country using XZY Agency. The funds were remitted to 22 individuals.

Mr. A declared that the funds transferred to Country Y were sent to his family members. However, the beneficiaries in Country Y were neither Malawian nationals nor the subject's relations. Moreover, the recipients' names reflected those of individuals from Country Y with no single name bearing the surname of A. Investigations established that Mr. A worked as a domestic worker for a home of people from Country Y. He was being used by the family to transfer money to Country Y.

Subsequent action

Investigations

Account closed

Case Study 2: Boarding customers on mobile platforms without their knowledge

Case description

A number of cases were reported to FIA of customers from a number of financial institutions who were defrauded through mobile payment methods. Several banks in the country have introduced their own mobile payment methods which connect customers' bank accounts to their phone numbers. The platforms allow customers to send/transfer funds to other accounts within their bank or to other banks. The platforms also allow the customers to access services such as; payments for utilities and subscriptions, request and pay for cheque books, apply for loans, pay for investment portfolio and insurance among others.

When the new mobile payment methods were introduced, existing customers were requested to express interest and apply/register to use the platforms. Not all customers responded to the requests. Fraudsters within the banks saw the opportunity to register inactive accounts for the services by providing their phone numbers or those of their accomplices. This enabled the fraudsters to transfer funds from the unsuspecting accounts to other accounts.

Subsequent actions

Administrative actions by the financial institution

Dismissal from employment of involved employees

Reimbursement of funds to defrauded customers

Arrests

6.7 Typology 7: Financial Institution Fraud; Fraud perpetuated or orchestrated by employees

Introduction

48. Between July 2020 and March 2022, several fraud cases were reported involving employees of financial institutions. Customers were swindled money which later led to the financial institutions incurring losses through reimbursements and restorations.

49. The fraudusters targeted dormant accounts or accounts held by customers residing outside Malawi. They were changing the customers' accounts credentials and details. The fraudusters were transacting in the accounts without the account holders' knowledge. In other instances, the employees linked phone numbers for mobile payments to a dormant bank account. The syndicate involved a number of employees within Malawi and foreigners proven to be the employees' relatives and acquaintances.

Cases summary

Offences	Theft, fraud, abuse of office
Customer	Individuals
Products & services	Cash, bank accounts
Channels	Transfers, cash withdraws

Indicators	• Understating deposited amounts in customer accounts. • Multiple movements of funds within a day between two destinations. • Lack of segregation of duties.

6.6.1 Case Study 1: Bank employee understating cash deposits by customers

Case description

Mr. D, a bank teller stationed at one of the remote branches of one commercial bank, was involved in theft of customer funds. He was targeting unsuspecting customers and those that were not frequently transacting in their accounts. Mr. D could either not enter deposit information into the customer's account or he credited lesser amounts than those deposited into the accounts.

The bank discovered the misconduct after 5 such transactions were made. In total, Mr. D swindled customers over MK8 Million. The matter was reported to Police and administrative action was taken against him. He was eventually dismissed and the bank paid back the swindled customers.

Subsequent action

Dismissal

Investigation

6.6.2 Case Study 2: Bank employees abusing an online payment system

Case description

A new trend was noted where funds were moved in and out of clients' accounts without their knowledge and consent.

XYZ Bank introduced a new product, a mobile payment platform. The platform has two tiers, one for customers and the other for agents. Commissions are earned by agents per transaction. Some XYZ Bank employees registered themselves or their relatives and acquaintances as agents. To earn higher commissions, the employees were moving funds back and forth from the dormant accounts of unsuspecting customers and agents. In some instances, multiple movements were being made within a day between accounts.

The innovation worked to the disadvantage of the Bank. It is highly likely that the Bank may not have undertaken a proper risk assessment of the product and did not put appropriate controls. The platform was reviewed and modalities were put in place to minimize the abuse.

Subsequent action

Review and implemantation of controls by the bank.

6.6.3 Case Study 3: Bank employee swindling cash recovered from fraudulent colleagues

Case description

A senior bank official, was entrusted to investigate a matter in which some fellow employees were suspected to have swindled funds from customers. The officers were suspected of committing fraud.

In the course of the investigations, the Official advised the investigated officers to refund the money they swindled so that there would be some leniency in the decisions following their actions. The Official advised the officers to pay back the funds in cash. Records were made for a repayment of MK3 Million in total.

However, the Official did not report the recoveries to the bank. Instead, he also embezzled the funds.

Administrative action was taken against the Official. He was subsequently dismissed from employment.

Subsequent Action:

Dismissal

6.8 Typology 8: Use of false documents

Introduction

50. The FIA also observed an ongoing trend on the use of false documents in carrying out financial transactions. This section will focus on the following areas where false documents were commonly used:

- Falsified funds transfers and cheques.
- Falsified documents to conceal ownership of the business.
- Opening and operating bank account with false documents.

6.7.1 Case Study 1: Using false documents to commit fraud

Cases Summary

Offences	Fraud
Customer	Businesses and individuals
Products & services	Cash, cheques, funds transfers
Channel	Remittances
Indicators	• Use of false identification documents. • Government funds being transferred without supporting documents.

	• Customers undertaking transactions that appear inconsistent with their profile and transaction history. • Large-value cheque deposits into newly opened bank accounts followed by immediate cash withdrawals once cleared. • Use of false identification to open bank accounts and conduct transactions. • Withdrawal in cash and transfer of huge amount of funds. • Large amounts of money being transferred to other accounts and individuals associated with this business.

Case description

Company A contracted Company B to make building materials for a lodge. As an advance pay, Company B received a cheque payment from Company A worth MK50 Million. Company B deposited a cheque with Bank X. The cheque was drawn at Bank Y. During the clearing process, the system at Bank Y unpaid the cheque automatically due to insufficient funds. Bank Y failed to notify Bank X of the unpaid cheque due to a technical problem.

As a result, Bank X credited the funds to Company B's account. After the account was credited, Company B withdrew MK45 Million leaving a balance of MK5 Million. It was later discovered that the cheque was fraudulent. Bank X recovered the remaining balance. Company A did not collect the remaining building materials from Company B.

The circumstances around which the fraudulent cheque was cleared, indicate connivance between the issuer of the cheques and the two banks by way of cheque kiting.

Subsequent action

Investigations

6.7.2 Case Study 2: Use of falsified documents to conceal business ownership

Case description

The FIA investigated a case where Person X had posed as Person Y from a foreign country to register and open an account for Company B. Person X worked as a Director of Government Department A and owned a business called Company C. In 2019, Company B opened an account with Bank G. When opening the account, the shareholders' names were provided as Person Y and Person Z. Person Z was a business associate of Person X at Company C.

Investigations established that information provided in the company's articles of association and the identification documents of the shareholders were both false. Also, Person X and Person Y were the same person. Person Y's full name was the middle name for Person X. In addition, the addresses and dates of birth provided for both X and Y were similar.

For one year, Company B received cheque payments amounting to MK200 Million drawn on Government Department A's account domiciled at Bank H. Notably, most of the cheque deposits into Company B's account were from Government Department A's account. The transactions were only conducted by Person Z. On the other hand, Person Y never transacted in Company B's account. A significant amount of the funds that was withdrawn from Company B's account

was later credited to the account of Company C and the personal account of Person Z.

Subsequent action

Investigations

Arrests

Restraining orders on property

6.7.3 Case Study 3: Misrepresentation to obtain funds illicitly

Case description

In 2021, Bank A received fund transfer instructions from Company X and Company Y amounting to MK100 Million and MK70 Million respectively. Person Z held two accounts with Bank B at Branch C and Branch D. Person Z was the beneficiary for both funds transfer instructions from Companies X and Y. Company X instructed that the funds be remitted to Person Z's account domiciled at Branch C whilst Company Y instructed that funds be remitted to Person Z's account domiciled at Branch D.

Bank A officials contacted the signatories for both Company X and Company Y to confirm the funds' transfer instructions before processing. The signatories for both companies advised the Bank that they never issued funds transfer instructions to remit funds to the said beneficiary.

It transpired that the funds transfer instructions issued to Bank A were made with an attempt to defraud the two companies. Person Z could have been a beneficiary of the attempted fraud. In addition, Person Z's account had never received such huge payments indicated in the funds transfer instructions since the account was opened.

Subsequent action

Close monitoring of transactions

6.9 Typology 9: Under declaration of KYC information by customers

Introduction

51. In the years 2020 to 2022, FIA noted an influx of STRs related to misinformation, hiding of information and under-declaration of customer information. Other STRs were as a result of comingling business transactions with personal transactions. As a result, STRs were being generated based on the mismatch of KYC information that customers provided when opening their accounts or updating their KYC information.

52. Information that customers usually hide or suppress is on; sources of income, level of expected turnover, whether they are engaged in businesses or other extra sources of income and the type of business they are engaged in. Other customers get evasive or violent when they are asked questions regarding the funds they are depositing into their accounts.

53. When preliminary inquiries were made on these STRs, it was found that the customers are engaged in very high intensive cash small scale businesses such as; sale of second-hand clothes, agricultural produce and grocery shops among others. Other STRs are generated on one-off large cash deposits which mostly turn out to be proceeds from the sale of land (it has been noted that there is an increase in the sale of customary land in areas around the cities of Lilongwe, Blantyre and Zomba).

54. On the other hand, some individuals use their personal bank accounts for business transactions. Confusion of eligibility and completeness of tax payable amounts by these businesses may arise due to comingling of personal and business transactions. This may also be abused as taxable

income may be understated, hence declaring lower tax than it was supposed to be.

55. Therefore, for individuals carrying out businesses, it would be advisable to open a business bank account.

6.8.1 Case Study 1: Using a personal account for business transactions to evade tax

Case Summary

Offences	Tax evasion
Customer	Individual, business
Products & services	Bank accounts
Channel	Bank transfers
Indicators	• Transactions did not match the type of account and declared information. • No other significant deposits into the account apart from the large funds. • Substantial increase in turnover in the account. • Abandoning the use of the business account for business transactions and opting for the use of a personal bank account.

Case description

There were a significant number of cases that the FIA analysed concerning the use of personal bank accounts for business. In one of the cases, Mr. G, a businessman, opened a business account with Bank A. He already had a personal account with the same bank. The bank noticed that he had started depositing revenue from his business into the personal account resulting in the dormancy of the business account. The total revenue into the personal account was MK453 Million in just under one year.

However, in his tax returns, Mr G declared a business account which did not have a reflection of the revenue earned from the business.

Subsequent action

Investigations

6.8.2 Case Study 2: Failure to update KYC information

Case description

The FIA received and analysed a case in which Mr. K opened a personal savings account with one of the commercial banks in 2013. For 4 years, modest transactions were going in and out of the account. The maximum transaction in the account was K200, 000. The declared business at the time of opening the account was a grocery shop with an annual turnover of K1 Million.

The trend in the account changed after the 4 years when the account was being regularly credited with large cash deposits. The funds were being deposited by various individuals from the City of Lilongwe. The deposits were being followed by immediate withdrawals of the same amounts, leaving a minimum book balance. Preliminary inquiries established that the customer was later engaged in rice farming, buying and reselling through retail and wholesale.

Subsequent action Investigations

7 EMERGING TRENDS

7.1 Typology 1: Use of Non Profit Organisations (NPOs)

Introduction

56. FATF defines a Non-Profit Organisation (NPO) as a legal person or arrangement or organization that primarily engages in raising or disbursing funds for purposes of; charity, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of good works. In the Malawi, NPOs are also referred to as Non-Governmental Organisations (NGOs). However, NPOs are vulnerable to ML/TF due to their access to different sources of funds and the trust they hold with the public.

7.1.1 Case Study 1: Use of NGOs to defraud the public

Case Summary

Offences	Money Laundering, fraud and theft
Customer	NGO individuals
Products & services	Electronic Funds Transfers (EFT), bank account
Channel	Remittances, mobile money transfers
Indicators	• Frequently move funds or other resources to offshore accounts. • Non registration of an NGO.

	• Collect funds from beneficiaries in form of registration fees before giving them aid. • Using false information and making false claims.

Case description

NGOs in Malawi are supposed to register with the NGO Regulatory Authority (NGORA) before they start operations. In 2018, a foreign NGO operating as a community-based organisation, established an office in the country. However, after 6 months of existence but before undergoing registration process with NGORA, the NGO started soliciting money from communities in rural and low-income societies while promising them various benefits.

FIA inquiries with NGORA established that the NGO started its operations in the country before registering as an NGO. The NGO was operating illegally and had been collecting money from unsuspecting underprivileged communities. The communities were swindled of funds in the form of registration fees for children education sponsorship and free agricultural inputs for farmers. After registration and payment, the purported beneficiaries of the NGO were not issued with any receipts or proof of payment.

This NGO also worked closely with local religious organizations and churches with the objective of convincing them that it will construct and renovate their churches, schools and health facilities. It also promised to sponsor pastors' children and promote agricultural activities in the member churches.

The NGO claimed that it had been registered internationally and that it gets funding from its mother body abroad. However, FIA did not find evidence supporting this claim. This NGO was successful in scamming the unsuspecting people because its name was similar to an already existing NGO. It also provided

false bank and mobile contact account details. Whenever people failed to pay for the subscriptions using the false bank account, they were asked to alternatively use the mobile account. This is how the NGO got the funds. Notably, the mobile money wallet number was in the name of a different organisation rather than the NGO.

Subsequent action

Ongoing investigations.

7.2 Typology 2: Layering of funds to create complex transactions

Introduction

57. Money laundering has three stages namely; placement, layering and integration. The placement stage is when illegal funds are introduced into the financial system. The second stage; layering, is to create multiple financial transactions to conceal the source and true ownership of the illegal funds. Layering is aimed at distancing the criminal proceeds from their source but target to present the criminal proceeds as clean by channelling the funds through different layers of transactions or financial instruments. Each layer presents legal participation in the financial system furthermore obscuring the illegal origin of the funds. Layering is believed to be the most complex stage of money laundering as it purposefully incorporates multiple financial instruments and transactions to circumvent AML/ CFT controls.

7.2.1 Case Study 1: Layering of funds

Case Summary

Offences	Money laundering
Customer	Individuals, businesses
Products & services	Cheques, cash, transfers, instructions, private banking
Channel	Banks, remittances

Indicators	• Moving funds between multiple banks or financial institutions or between accounts within the same bank. • Converting cash into financial instruments such as cheques. • Frequent transactions with large sums. • Deposits of funds into accounts that are then rapidly withdrawn or transferred. • Not fully disclosing the source and destination of funds. • Large number of transfers between a group of individuals and accounts made in a systematic way.

Case description

In the year under review, the FIA reviewed a case in which three brothers Messrs. X, Y and Z owned three companies between them. The three companies were engaged in different kind of businesses. The businesses included; transportation for Company A, selling of eggs for Company B and selling of fertilizer for Company C. All the businesses' bank accounts were held at Bank A. Messrs. X and Y were the only signatories for the business accounts and managed to do every transaction through private banking.

Company C opened an account with Bank A in March 2020. It declared that it was in the business of selling fertilizer with an annual turnover of K5 billion. Through

analysis, it was noted that most of the transactions happening in the account were foreign currency transactions. Furthermore, immediately after funds were transferred into the account, there were followed by outward SWIFT payments. The purpose for these transfers was for the purchase of fertiliser. This pattern started soon after the account was opened. The company went further to open two more bank accounts, one of which was a call deposit account.

Between the months of November and December 2020, transactions involving high value transfers were made from one business account to the other. Transfers could be done from the eggs company, then to the transport company, then the fertilizer company. The purpose of the transfers was not disclosed. The fertilizer company would then draw a cheque that was later withdrawn as cash in the transportation company. On some days, there were funds transfers into the personal accounts of Messrs. X, Y and Z. The pattern of how the transactions were done did not make any business sense despite the transactions appearing legitimate.

From the pattern observed, the movement of funds indicates a large number of transfers between a group of individuals and accounts which were being made in order to layer the funds.

Subsequent action

Investigation

8. PREVALENT TRENDS

8.1 Typology 1: Fraud

Introduction

58. Fraud is when an individual knowingly misrepresents the truth or conceals a material fact for one's own advantage or to cause another a loss. Fraud encompasses a wide range of behaviours that are linked, from trickery to deceit, with the intention of making a gain. Under this typology, the first case study is on corporate identity fraud, where an organisation's corporate identity was used to open an account to obtain services by deception. The second case study is on fraud by abuse of position.

8.1.1 Case Study 1: Corporate identity Fraud

Case Summary

Offences	Fraud, theft
Customer	Individual, businesses
Products & services	Electronic Funds Transfers (EFT), bank account, ATM withdrawals
Channel	Banks
Indicators	• Using a fraudulent account name. • Frequent large cash deposits not in line with account profile. • Large cash and electronic funds transfer after funds deposits.

Case description

The FIA received and analysed a case in which Mr. W opened a bank account for NGO M at a branch of Bank Y. The KYC documents indicated that the purpose of the NGO was to conduct fundraising activities to support vulnerable communities across the country.

After 2 years, another branch of Bank Y received a complaint from an individual, Mr. X, who claimed that he initiated a transaction to transfer funds amounting to MK1 Million into NGO M's account.

Mr X later discovered that the funds did not get into M's account. It was later established that Mr. W intentionally opened a bank account with a similar name and at the same branch with the legitimate NGO to fraudulently profit from the donations from well-wishers. Consequently, Mr. W was requesting and collecting assistance from well-wishers by using details of the legitimate M NGO account but with a different account number. Large sums of cash were being deposited into the fraudulent M's account followed by immediate withdraws and purchase of foreign currency. The funds were later being transferred to several personal bank accounts. The funds involved were more than MK8 Million.

Subsequent action

Investigations

Freezing of bank account

8.1.2. Case Study 2: Theft by trickery

Case Summary

Offences	Fraud and theft
Customer	Individual
Products & services	Electronic Funds Transfers (EFT), bank account, ATM cash withdrawals

Channel	Banking
Indicators	• Frequent large cash deposits not in line with account profile. • Large cash and electronic funds transfer after funds deposits. • Large funds withdrawals. • Immediate funds transfers/withdrawals from the entities' account following fund deposits.

Case description

The FIA received and analysed a case in which Mr. X operating as a cross-border transporter lost items belonging to his client, Company W, whilst in transit from South Africa to Malawi through theft in May 2020. Mr. L, operating as a freight agent, offered to assist with the recovery of the lost items through black magic. He asked Mr. X to deposit MK30 Million into his account to provide information leading to the recovery of the stolen items.

On 4 June 2020, Mr. X deposited a sum of MK30 Million into Mr. L's bank account at Bank Y. The amount was withdrawn on the same day. After six days, Mr. X discovered that Mr L had disappeared and could not be reached on his mobile phones. In a quest to recover his money, Mr. X went to the bank where Mr. L account was held for further inquiries.

Subsequent action

Investigations (Mr. L still at large)

8.1.3 Case Study 3: Impersonating LEA Officer to defraud the public

Introduction

59. The FIA observed the recurrence of an old trick (419 Fraud) where members of the general public were scammed into believing that they could be part of an investment portfolio belonging to foreign investors. The fraudsters would trick unsuspecting victims into believing that for the investment funds to be accessed, the foreign funds must have been cleared through several processes locally and that these processes had to be paid for. The fraudsters went as far as impersonating law enforcement officers, bank officials and clearing agents to convince the victims to release money to clear the purported investment funds.

Case Summary

Offences	Impersonating public officers, fraud
Customer	Individual
Products & services	Bank accounts, cash, EFTs, ATM cards,
Channels	Mobile money remittances
Indicators	Instant withdrawals at merchant POS soon after large cash deposits or EFTs.

Case Description

Mr. C was defrauded of MK20 Million. He was approached by Mr. D who convinced him that some foreign investors were ready to partner with him to construct a manufacturing company within his area. Mr. D convinced Mr. C that the foreign funds were being held by clearing Company A and that before they could access the funds, they had to get clearance from RBM and FIA.

Mr. D connived with his associates who posed as officers from RBM, FIA and Clearing Company A. Mr. C was convinced that the people he was dealing with

were *bona fide* officers and went ahead to pay the requested amount in order to access the foreign funds. He believed the expected funds to be USD 250,000.

He consequently sent the money to the fraudsters at different intervals, believing that he was sending to the mentioned institutions. The total amount sent was MK20 Million. After the last payment, he realised he had run short of funds yet the associates were still requesting for more money. He decided to visit the institutions in person in order to plead his case. However, upon hearing that the institutions did not provide the services he had paid for, he realised that he had been duped and that the people he was dealing with were impersonators.

Subsequent action

Prosecution

8.2 Typology 2: Tax evasion

Introduction

60. Tax evasion is the non-payment or underpayment of legal taxes. It may be achieved through falsification of declarations or non-declaration of income or value for duty at all. An individual may declare less income, profits and gains received by or accrued to them from a source within or deemed to be within Malawi, than the amounts gained. In other cases, tax evasion may be achieved through overstating deductions to declare losses. As far as tax obligations are concerned, it is important to note that all registered companies in Malawi are obligated to pay tax. Tax is applicable on all income earned in a year, less allowable expenses and allowances.

61. The success of tax evasion depends on the ability to disguise the financial trail of taxable income. In tax evasion, taxable income is concealed from detection by the tax authorities. The evaded tax proceeds are transformed

to appear legal in money laundering. From the STRs received in the period, a trend was noted where taxable proceeds were being deposited into personal bank accounts to evade tax. Also, businesses did not disclose or falsified documents to evade tax.

8.2.1 Case Study 1: Corporate tax evasion

Case Summary

Offences	Tax evasion
Customer	Business
Products & services	EFTs and bank account
Channel	International Trade
Indicators	• Provision of fictitious information. • Misclassification of goods. • Conducting business transactions in personal bank accounts. • Making false declarations. • Under-declaration of imported goods.

Case Study 1

In May 2021, one of the LEAs arrested directors of Company X on allegations of tax evasion. The estimated amount lost through tax evasion was MK15 Billion. The arrests were done after the LEA had conducted a tax investigation on the Company.

The Company managed to evade tax through several methods. Firstly, the Company under-declared revenue. That is, revenue was realized but the Company could not declare the actual revenue realized for tax purposes. This

had an impact on Value Added Tax (VAT) and income tax remitted to the Malawi Revenue Authority.

The second method was through non-payment of customs duty. The Company smuggled already finished products into the country and declared them as raw materials, thereby, not paying tax. However, the Company went ahead and sold the imported finished products.

The third method was an underpayment of Pay as You Earn (PAYE) tax remittance in respect of monthly earnings to expatriates. The Company had expatriates employed by the Company and were paid accordingly. However, the Company was not paying the correct PAYE for this category of employees.

Subsequent action

Arrests

Seizures

Prosecution

Case Study 2

The FIA received and analysed a report concerning Mr. XY, a business person owning and operating Company Z. The Company has business accounts with several banks. Mr. XY also has personal bank accounts with several banks in the country. At Bank A, it was noted that cheques that were meant to be deposited into the business account were deposited into his personal account at the same bank. Following the cheque deposits, transactions were made concerning the business account such as payments to suppliers of Company Z and purchases of additional motor vehicles for the Company.

Since the revenue realised was not being deposited into the business account, the account was always in overdraft. This scenario provided Mr. XY with an explanation as to why he was not utilizing the business accounts for Company Z's

business transactions. For a period of one year, funds amounting to MK1 Billion from customers of the business were deposited into the personal account of Mr. XY. In conclusion, this was tax evasion through understating of business revenue resulting in the declaration of losses that were not taxable or under-declaration of taxable profits.

Subsequent action

Tax investigations

PART D: RECOMMENDATIONS

62. As earlier stated, this report offers insights into financial crimes trends and methods that are being used by individuals in the financial sector. These trends and techniques are shared with relevant stakeholders such as financial institutions in order for them to be on the look out for red flags and indicators; law enforcement agencies in order for them to focus on areas of interest in their investigations; sectoral regulators and other policy drivers so they can guide policy objectives in addressing the issues raised in relation to the trends and methods of financial criminality. The general public is also empowered to be alert on various techniques used by criminals to either scam them of their money or indeed use them to launder proceeds of crime or finance terrorist financing. Below are some recommendations based on the information that has been shared:

9.1 Improved Enhanced Due Diligence for customer information

63. Reporting institutions should ensure that Enhanced Due Diligence (EDD) should be conducted and results documented for customers in accordance to their risk profiling.

64. As noted earlier, a significant number of STRs that the FIA receives from banks, are based on the fact that the customers' details are not updated to match their current economic situation. As a result, any mismatches between current customers' transactions and their KYC information on source of funds, and expected income in the account, results in the reporting of an STR to FIA.

65. On this issue, financial institutions note of the challenges experienced when drawing the line between tipping off and asking questions necessary for KYC updates. The other challenge emanates from customers hiding information from their business activities. The trend of reporting legitimate transactions as suspicious has been a growing concern for the FIA. There

are instances where financial institutions reported over 200 STRs on cases that merely required updating of KYC information.

66. Therefore, FIA's concern is on the quality of some STRs that financial institutions prepare. Some focus on suspicions that could be easily substantiated by obtaining correct and up-to-date KYC information.

9.2 Improved Transaction Monitoring Systems

67. Financial Institutions should enhance their transaction monitoring systems in order to easily identify changes and unusual transaction patterns. This may also assist reporting entities in risk assessment, hence resulting in implementation of appropriate mitigating factors.

68. Effective transactions monitoring systems may not only assist with the identification of red flags, trends and patterns but also give rise to further monitoring.

9. 3 Risk assessment before launch of new products

69. The reporting entities should ensure that they conduct AML/CFT risk assessment on all new products prior to their launch. This will clearly identify the risks associated with the products resulting in the implementation of appropriate mitigating factors to such risks.

9.4 Enforcement and adherence to control environment by governmental MDAs

70. The control environment in governmental Ministries, Departments and Agencies (MDAs) should be effective and efficient to curb loss of public funds. The controls should be efficient enough to prevent fraud, corruption, theft and other financial crimes. In addition, they should also detect and

deter any override and mismanagement of such controls by all responsible employees.

71. To ensure that the employees are all aware, they should be trained and encouraged to take ownership of these controls. Ethical values, such as integrity and mind-set change, should be at the heart of all employees in these MDAs.

9.5 Improved AML/CFT control in NGO sector

72. All NGOs engaging in the solicitation or receipt of money, goods or property for charitable purposes should be required to obtain a licence and register with the relevant authorities before starting operations. Further, all players in this sector should make information regarding their operations publicly available. Financial information should be issued in terms of financial statements and should provide details of income, its source and the expenditures for the relevant period.

73. As noted earlier on controls, the same applies to this sector. Appropriate controls should be implemented to ensure that all funds are fully accounted for, spent in a manner consistent with the purpose and objectives of the NGO's stated activities. On the other hand, the NGORAand other relevant authorities should ensure that the NGOs are screened for due diligence purposes before they are registered and issued a licence.

74. Furthermore, the general public should be encouraged to report any NGO to law enforcers in the event of any suspicious activities noted in relation to the particular NGO. In addition, all NGOs are supposed to be monitored by relevant regulators on issues relating to AML/CFT.

9.6 Public Private Partnerships in AML/CFT

75. All stakeholders and private sector bodies involved in AML/CFT should engage concerted efforts in bringing awareness on financial crimes to the general public. For example, the public should be made aware not to share very confidential information such as; identity, Personal Identification Number (PIN), mobile account numbers as well as bank account numbers as a control against fraud.

76. There should also be efforts made towards exchange of information leading to the prevention, detection and deterrence of these crimes. The efforts will help in the reduction of costs associated with financial crimes. Besides, the sectors should ensure that all the interventions in AML/CFT efforts follow the Risk-Based Approach. This will help in intentional resource allocation when responding to the evolving risks associated with financial crimes.

9. 7 Control of cross-border currency declaration

77. Authorities should consider monitoring and evaluating the current implementation of foreign exchange controls.

78. Secondly, there should be awareness to the general public not to allow third parties to use one's visa or debit cards.

79. Thirdly, there should be enforcement of declaration of currency at points of entry and exit. Finally, the government should consider reviewing policies, to allow use of the Malawi Kwacha for cross-border trade and acceptance of the currency by other countries

80. In as much as accessing of forex at the border districts is concerned, the trend and pattern observed so far may raise a concern of abuse of foreign

currency transactions. This may also create a loophole for terrorist and proliferation financing.

9.8 Mobile Money and SIM cards registration

81. The government through Malawi Communications and Regulatory Authority (MACRA) should come up with legislation that will limit the number of Subscriber Identity Module (SIM) cards an individual or entity can hold. There is need for stringent controls on replacement of lost and registration of new (SIM) cards.

9.9 Cash Transaction

82. Government should consider a law or policy to limit cash transactions and cash withdrawals from financial institutions. Emphasis should be made on the need to utilise account-to-account transfers and use of electronic payments involving large transactions instead.