FINANCIAL INTELLIGENCE AUTHORITY

With a vision for a financial crime-free Malawi

MONEY LAUNDERING TRENDS AND TYPOLOGIES REPORT 2018-2019

Table of Contents

1 PART A: GENERAL INFORMATION

GENERAL INFORMATION

FIA general information

Registered name	:	Financial Intelligence Authority
Postal address	:	Private Bag B441,Capital City ,Lilongwe, Malawi
Telephone number	:	+265 1 759 141
Fax number	:	+265 1 759 151
Website	:	https://www.fia.gov.mw/
Email	:	info@fia.gov.mw

1.1 ACRONYMS AND ABBREVIATIONS

Abbreviation	Definition
AML/CFT	Anti-Money Laundering/ Combatting Financing of Terrorism
BEC	Business Email Compromise
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
FAFT	Financial Action Task Force
FCA	Financial Crimes Act
FIA	Financial Intelligence Authority
KYC	Know Your Customer
LEA	Law Enforcement Agency
ML/TF	Money Laundering/ Terrorism Financing
NPM	New Payment Methods
STR	Suspicious Transaction Report

1.2 INTRODUCTION

It is a known fact that the nature of money laundering and terrorist financing (ML/TF) crimes and other financial crimes is continuously shifting. Criminals are taking advantage of the advancement in technology and digital-driven financial services to undermine the anti-money laundering (AML) and combatting of terrorist financing (CTF) regimes. Such advancement on the part of criminals is rendering it more complex to deter, prevent and detect criminal activities.

The Financial Intelligence Authority (FIA) Malawi is increasing its efforts to adapt to these continuous changes and come up with measures that would help in creating *a financial crime free Malawi.* As part of such efforts, the FIA continues disseminating financial intelligence to law enforcement agencies (LEAs) and other relevant stakeholders.

Production and dissemination of strategic intelligence is one measure that the FIA has in place to allow stakeholders and the public to take proactive actions towards fighting ML/TF. The ML/TF Trends and Typologies report is part of the strategic intelligence that the FIA produces and disseminates.

By developing this report, the FIA endeavors to be a source of knowledge, guidance and best practices on ML/TF crimes and other financial crimes, to protect customers and businesses in the financial system. The trends and typologies presented in this report will strengthen various sectors' ability to detect and counter the threat of financial crimes including; money laundering, terrorist financing, bribery and corruption, tax evasion, business email compromise, and market manipulation.

As LEA's, various stakeholders and the public access this report, the FIA is confident that it will continue to inform them of the various financial crimes, and they will take a proactive and robust stand against financial crimes and their negative impact. This will contribute to the integrity of Malawi's financial system, thereby contributing to the growth and development of our economy.

1.3 EXECUTIVE SUMMARY

FIA's 2018/2019 Trends and Typologies report tackles a number of areas that include new and emerging areas such as; Business Email Compromise (BEC), foreign exchange law violations and money laundering through insurance products or services. In addition, there have been continuing trends in environmental crimes, foreign currency externalisation, insurance fraud and theft of public funds. It is important to note that typologies relating to environmental crimes have not be discussed. This is because there will be another typology report that will be produced in 2020 specifically on environmental crimes.

The notable emerging trends in this report are ML using Business Email Compromise and new payment methods (NPM). BEC is a type of scam targeting companies and individuals who conduct wire-transfers and have both domestic and international suppliers of goods and services. Private and public institutions, individuals and publicly available email accounts of targeted executives or high-ranking finance executives and those involved with wire-transfer payments are either spoofed or compromised through a number of mechanisms to carry out fraudulent financial transfers, resulting in losses in millions of Kwachas. In Malawi, the past two years have seen fraudsters stealing millions of Kwachas from institutions and individuals by compromising their official email accounts and using those accounts to initiate fraudulent wire-transfers. On the other hand, NPM are payment methods that are used in the modern business world that include online payments, bank transfers and other online services used for payments.

Therefore, it is important for users of these channels to be cautious of these and other online scams such as phishing and spoofing in order to avoid loss of funds. In most cases, the fraud goes beyond international boundaries, making it too cumbersome and costly for victims to pursue the recovery of lost funds. More importantly, apart from individuals, financial institutions should also be cautious of these types of frauds so that they should not end up unknowingly being associated to ML and TF. In this regard, the FIA has taken efforts to trace and recover the lost funds. However, due to the nature of the scheme, it is very difficult to recover all the funds because the perpetrators withdraw them in real time. The FIA has also encouraged financial institutions to conduct enhanced due diligence (EDD) when handling non face-to-face transactions.

Furthermore, by our core function of detecting, preventing and deterring money laundering and terrorist financing (ML/TF), we believe it is important for the general public, financial institutions, LEAs to be aware of Business Email Compromise type of fraud that is on the increase in Malawi and adopt mitigating measures so that they are able to safeguard themselves from significant loss.

Illegal externalization of foreign exchange and access to foreign exchange notes for sale on the informal market remain the notable ML trend over the years. In the previous report, the modus operandi was the use of false Malawi Revenue Authority (MRA) value of

imports declaration, Form 12, for over and under-invoicing. Currently, due to the interventions by FIA, Reserve Bank Malawi (RBM) and MRA, there has been a significant decline in the use of these methods. One of the interventions involved granting financial institutions access of MRA database to verify import documents. The current report shows that the perpetrators of illegal externalization connive with bank officials who make it possible for transactions to be conducted without supporting documents, duplicating documents and transactions. Another modus operandi is the externalization of funds through cross-border movement of currency. So far, there have been a number of interceptions by the Malawi Police Service (MPS) at the ports of entry and exit.

From the foregoing, FIA has been encouraging financial institutions to corroborate import documents with MRA, do lifestyle audits on their employees, and design and implement appropriate controls that mitigate the risk of collusion such as segregation of duties, compulsory holiday, staff rotation and appropriate reviews and approval of transactions by independent staff.

This report also highlights trends related to insurance fraud and theft of public funds. The implementation of the Pensions Act in 2011 has brought with it some structural changes in the pension's funds management sector. Significant changes include the mandatory contributory pensions for all workers in Malawi. The pension fund administrators have become a target by unscrupulous individuals. The report will show how the fund administrators have been defrauded through cloned cheques and payments to ghost beneficiaries. The fraudulent payments appear to be enabled by insider who connive with these unscrupulous individuals to defraud their companies.

On theft of public funds by public officers, it has been noted that unlike in the previous years where pension fund accounts were targeted, for the period under review, the target was on salaries account. The FIA noted that public officials override controls in order to have access and insert ghost workers onto pay rolls and later launder the funds either through self-laundering or use of third parties. Some of the reasons that may be attributed to this scam are insufficient monitoring and audit controls in government departments and failure of the payment system in financial institutions to cross-match account numbers and names resulting in the creation of an opportunity for the diversion of funds to the accounts of the fraudsters.

2 PART B: OVERVIEW OF THE SUSPISCIOUS TRANSACTION REPORTS (STRs) RECEIVED

2.1 Overview of the Suspicious Transaction Reports (STRs) Received, Analyzed and Investigated

This section gives a general overview of the STRs, which the FIA received from reporting entities, analyzed, investigated and disseminated to law enforcement agencies. STRs are a vital source of information in identifying funds that may be used for terrorism, criminal and other illicit activities. This section, therefore, appraises the reporting institutions on the criminal patterns and trends that FIA has identified in the course of its analysis of the STRs and financial investigations. These indicators will significantly assist the financial institutions in developing an effective anti-money laundering (AML) regime to prevent individuals and criminal organizations from using financial institutions to launder proceeds derived from crimes. Further, the identified indicators will help law enforcement agencies to develop better investigation techniques to combat ML/TF and other financial crimes.

The information from this report has been derived from the following sources:

- STRs that were received and analysed from the various reporting entities for the fiscal year from July 2018 to June 2019. During this period, a total of 16 reporting entities filed STRs with the FIA. The total number of STRs was **313**. The banks submitted **286** of the STRs representing 91%. The remaining **27** were from the insurance sector, foreign currency exchange bureaus, accountants, mobile money operators and independent.
- Requests for information and other information from law enforcement agencies.
- Media reports and other open sources information.
- Information available to the FIA from other FIUs or similar institutions.

2.2 General Observations from STRs and Financial Investigations

2.2.1 Common / Prevalent Indicators observed

- Substantial increases in cash deposits without apparent cause subsequently transferred into other bank accounts and withdrawn from the account within a short period of time out of the account.
- Deposits or withdrawals of large amounts of money, which are significantly inconsistent with the customer's usual transactions, income or status, or business activity.
- Transfers of large amounts of forex to foreign jurisdictions without supporting documents.
- Individuals or companies submitting forged and false documents to banks for application of forex with intention to externalize the funds. The most forged documents include invoices from suppliers, import documents and travel

documents. Travel documents include use of travel agents to issue tickets that are immediately cancelled once foreign currency has been obtained.

- Reluctance by customers to provide full and accurate information when opening an account. In addition, some clients provide minimal or fictitious information when applying to open an account or providing information that is difficult for the institution to verify.
- Individuals or company profiles not matching with the transaction trends. For instance, a personal bank account receiving or disbursing large sums of money, which have no obvious purpose or relationship to the accountholder.
- Collusion between customers and bank officials to falsify import documents which allow the customer to make multiple international payments using the same import documents. Customers present duplicate import documents, which have already been used at multiple banks and in some instances at the same bank at an earlier date.
- Using cloned cheques to defraud, issuers of the cheque, the bank and beneficiaries. Usually there is collusion between fraudsters and employees from the pension fund management institutions. This has been prevalent in the insurance industry where cheques for beneficiaries are targeted.
- Multiple large cash deposits made at service centres based in the border districts followed by immediate withdrawals and purchase of forex in the cities or towns. This trend is associated with illegal foreign currency trade market also known as black market.
- Use of third parties such as relatives and friends to receive or transfer funds.
- Import payments to suppliers whose business does not match with the business of the importer.
- Frequent purchase of forex/ travel allowance for a business that virtually does not require forex or frequent business travels abroad.
- Large sums of cash deposits from multiple sources into a newly opened account followed by immediate international transfer/ application for forex purchase.
- Opening of parallel accounts bearing names similar or close to existing account names with an aim of diverting funds meant for the existing bona fide accounts.
- Failure of financial institutions to conduct a comprehensive know your customer (KYC) and customer due diligence (CDD) which result in obtaining incomplete information of the client when establishing business relationships.
- Internet facilitated theft. The imposters obtain key details of the victim by hacking an email and directing the victim to make a payment into the account of the imposter.

- Bank employees remitting funds on behalf of foreign nationals who lack appropriate documents.
- Several individuals or companies whose nature of business is virtually different making international funds transfers to the same beneficiary for the same raw materials. For instance, customer who owns a shoe manufacturing company and a customer who owns a wholesale shop of plastic shoes and umbrella, making international payments to the same beneficiary for the importation of shoe making machine.
- Sale of large sums of forex whose source is unclear or disguised as proceeds from sale of farm produce across the borders of Malawi.
- Unwillingness of customers to furnish financial institutions with further information when requested to do so and triggering termination of business relationship.
- Customers providing falsified financial account to obtain facility/loan from financial institution.

3 PART C: MONEY LAUNDERING METHODS AND TECHNIQUES

3.1 MONEY LAUNDERING METHODS AND TECHNIQUES

The FIA reviewed and analyzed the suspicious transaction reports and requests received in the 2018/2019 financial year from which it observed on-going and declining money laundering methods and techniques. Further, in this report, the FIA has particularly noted that theft of public funds and exchange control violations continue to top the list as major predicate crimes for money laundering in Malawi. In addition, the weaknesses highlighted in the payment of salaries and pension continue to provide opportunities that are exploited by corrupt public officials to embezzle public funds, which are laundered via themselves or third parties. Bank accounts of third parties are used to make and receive payments of embezzled public funds, and recipients of the embezzled funds channel back the funds to the corrupt public officials through cash withdrawals or transfers to the accounts of the corrupt public officials.

An important observation in this typologies report relates to high numbers of suspicious transactions involving payment of pension by insurance companies through financial institutions that are used as payment channels. The cases involving pension related money laundering have shown that the insurance sector is significantly used by corrupt insurance officials to launder embezzled public pension funds. With an increase in public pension funds since the coming into force of the Pensions Act in 2011, the Pension fund administrators are being targeted because of the numerous pension payments being processed. The methods mainly used are cloned cheques and insertion of ghost pension beneficiaries on the payroll.

Another important observation is the emergence of new money laundering trends. These are fraud through Business email compromise (BEC) and new payments methods (NPMs). BEC is part of a criminal scheme that uses the cyber space to defraud unsuspecting people in Malawi. Methods used include hacking into victims' email accounts and addresses. The emails appear as if they were sent from a trusted source when in real sense they were sent from a different account by a malicious actor.

NPMs related money laundering methods included fraudulent claims by agents providing Point of sale machines (PoS) and conspiring between agents and card holders to generate false transactions. The use of NMPs is slowly becoming attractive in Malawi because of easy access to funds and avoidance of risks associated with carrying huge amounts of cash. However, reports show that it is also creating new opportunities for criminals across the globe to misuse such technology for money laundering and terrorist financing. However, contrary to the use of cash, NPMs have the advantage of generating electronic records which provide investigative leads to Law Enforcement Agencies.

3.2 CONTINUING TRENDS

3.2.1 Exchange control violations

- Connivance between bank officials and Customers to illegally externalize foreign currency by making international money/wire transfers without supporting documents.
- Bank customers applying for foreign travel allowance using fake documents.

3.2.2 Theft of public funds

- Corrupt public officials creating ghost loan beneficiaries to launder public funds.
- Corrupt public officials paying themselves huge and irregular salaries.
- Corrupt public officials using third parties and associates to launder proceeds of crime and conceal ownership of funds.
- Corrupt public officials using their bank accounts to launder proceeds of crime.

3.2.3 Insurance Fraud-creation of fake beneficiaries

- Insurance officials cloning cheques which are paid to illegimate pension beneficiaries.
- Insurance officials inserting ghost pension beneficiaries on the payroll.

3.3 EMERGING TRENDS

3.3.1 Business email compromise (BEC)

- Fraudulent emails directing the transfer of money via electronic transfers.
- Emails directing victims to wire money to specific bank accounts.

3.3.2 Use of new payment methods

- Fraudulent claims by merchants using Electronic Point of Sale (POS) devices.
- Collusion between Debit/Credit cardholders and merchants through POS machines to fraudulently make false payments.

4 PART D: MONEY LAUNDERING TRENDS AND TYPOLOGIES IN MALAWI FOR THE YEAR 2018 TO 2019

4.1 MONEY LAUNDERING TRENDS AND TYPOLOGIES IN MALAWI

4.1.1 Typology 1: Exchange Control violations

4.1.1.1 Introduction

In Malawi, the Exchange Control Act provides for the administration of foreign exchange. However, the FIA has observed that there are exchange control violations, which result in illegal currency exchange for the purpose of laundering the proceeds of crime. The 2017/2018 Trends and Typologies report, noted of illegal purchase and illegal externalization of foreign currency as one method used in ML, and this report shows that this method is still in use.

Case summary

Offence	• Illegal externalization of foreign currency • Money laundering • Uttering of false documents • Exchange Control violations,
Customer	Private customer
Products and Services	• Wire-Transfer, • Foreign Currency notes • Cash withdrawals
Channels	ATM, Cheques, Foreign exchange, travel allowance
Indicator	• Frequent wire-transfers from several individuals to one recipient • Declared business activity not making economic sense as compared to the account transactions • Accessing foreign exchange without corresponding business requirements or documents • Collusion between bank staff and foreign nationals • Lack of appropriate controls such as segregation of duties, proper reviews and approval of transactions.

4.1.1.2 Case Study 1: Exchange Control violations through illegal externalization of forex

In 2018, the FIA discovered illegal foreign exchange schemes by Mr. Lennox, a customer of a local bank. Mr. Lennox (not his real name) was receiving numerous wire-transfers from five individuals from a neighboring country Z. The five individuals were using a wire transfer platform available at bank X that has branches in country Z and Malawi.

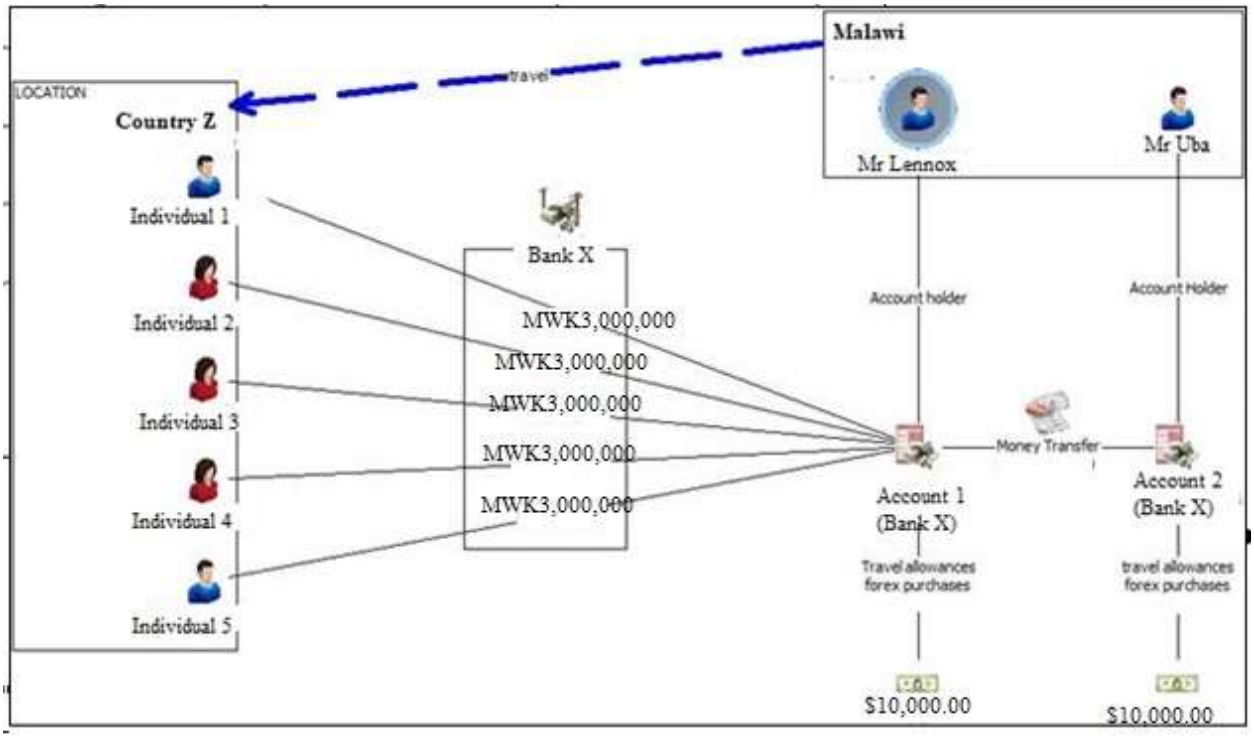
The current financial situation in country Z is a delicate balance where the US dollar currency note is in high demand against the less desirable local currency. The scheme involved sending money within the allowable threshold between country Z and Malawi. Mr. Lennox received over 100 wire-transfers totaling nearly K40 million. Mr. Lennox informed the bank in Malawi that the funds were proceeds of sales of building materials by him to the five individuals in country Z. Mr. Lennox would in turn buy US currency notes from bank X which were collected by one of the five individuals transferring funds from country Z to Malawi.

Mr. Lennox would also make cash withdrawals and transfers from bank X to other individuals within Malawi. Notable transfers were made to Mr. Uba (not his real name) who used the money to buy US currency notes of nearly US$10,000.00 for travel to Dubai and Country Z. Mr. Uba further made payments to an accommodation establishment in Blantyre for a nominee of the five individuals in country Z. the nominee was purportedly in Malawi to collect US dollar notes from Mr. Lennox and Mr. Uba.

The scheme violated foreign exchange controls in both Malawi and country Z. A disclosure was made to authorities in country Z, who are investigating the matter further. The source of funds in Country Z was not known by the time this report was published. Important to note is that in Malawi, the case is ongoing.

The scheme is depicted in the following Chart:

Case study 1: The chart visualizing the movement of funds from country Z into Malawi and back to country Z



4.1. Case Study 2: Collusion between bank officials and businesses to allow illegal transactions

The FIA became aware of a syndicate where officials of a financial institution colluded with foreign nationals to externalize over K4 billion within a period of one and a half months without supporting documents. The syndicate involved about ten accounts belonging to different individuals all held in Bank M.

The funds were externalized to country C without the requisite documentation, such as invoices and personal identification information in the system. The transactions were purported payments for imports. During preliminary enquiries by the bank's international trade department, it was found that there were no reports and documents of the transactions. Staff charged with the responsibility of inputting and authorizing the transactions feigned ignorance and blamed it on the system. The concerned staff quickly tried to recall the last batch of funds without being asked by authorities in the bank.

Accounts involved in the syndicate were frozen and staff involved are under investigation. The FIA's investigations established that:

- there were no supporting documents for the transactions.
- the transactions were done by staff who were not authorised to carry out such transactions.
- there was connivance between bank officials and the businesses involved.
- bank officials manage to override foreign currency exchange rates and transfer the funds at a lower rate which resulted in losses.
- The foreign nationals were being investigated for ML and the bank officials were dismissed.

4.1.2 Typology 2: Money Laundering using Business Email Compromise

4.1.2.1 Introduction:

The purpose of this typology is to highlight some of the techniques which criminals use to infiltrate emails and network systems of organizations and individuals. The malpractice is achieved through impersonation of key contacts and decision-making officials to deceptively obtain sensitive information from them. This enables the criminals to send instructions through hacked victim's email account and address with an aim of obtaining financial benefits. This process is called Business Email Compromise (BEC) fraud scheme.

In 2018, the FIA observed that there is an increase in the number of Malawians losing money through fraudulent transfers of funds using wire-payments initiated and instructed through email system. These acts have been noted to be targeting Malawians who are buying goods from overseas.

In Malawi, common cases have involved fraudsters using the internet to gain details of bona fide overseas suppliers and creating email addresses that are similar to those of the suppliers. The fraudsters then send fraudulent emails posing as the as the supplier's contact persons. In the emails the request prospective customer to make an urgent funds transfer using revised banking details.

It has been discovered that the fraudsters aim at tricking recipients of the email into believing that they are dealing with the bona-fide supplier who first contacted them because the changes in email addresses and email content are so miniscule that only skilled reviewers or systems may immediately detect the differences.

Case Summary:

Type of Offence	Money Laundering and Fraud by business email compromise, cyber-crime, impersonation
Customer	Individual, corporate
Product and Services (Instruments and techniques)	Electronic Funds Transfer, internet banking
Channel	Interbank transfer
Indicators	• Unusual changes of payment instructions • Fraudulent internet transfers • No apparent relationship established between sender and beneficiary • Transfer to high risk jurisdictions where it is difficult to recover stolen funds due to weak AML regime. • New instructions sent from the same email address requesting the fraudulent wire transfers • Use of money mules to remit funds offshore

4.1.2.2 Case Study 1: Fraudulent Wire Transfer through impersonation

In 2018, the FIA established that there was a Malawian national who engaged a motor vehicle dealer in country GH to supply him with a motor vehicle. After the deal was made, the buyer received an email which appeared to be from the bona fide motor vehicle dealer he had earlier engaged instructing him to urgently transfer the funds using new bank account details to a bank held in Country Y. The email with the new bank instructions was actually from a fraudster, who created an email address which resembled that of a bona fide supplier – impersonating a known contact person from the overseas car supplier.

The buyer did not notice the difference in email addresses and went ahead instructing his bank through a series of emails to transfer funds to the bank account provided in the email.

The fraud was discovered after the real motor vehicle supplier in country GH emailed the buyer asking for payment on the order. It was discovered that the bona fide supplier had never emailed the buyer nor supplied him with a revised invoice to transfer the funds to a different bank account in country Y. Investigation revealed that the payment had instead been made to the fraudster's account in country Y, following a breach of supplier's email system.

The FIA engaged with the FIU in country Y to locate the beneficiaries and destination of the funds. The FIA learned that the funds were withdrawn immediately after the transfer

was done. Further, the FIU in country Y informed the FIA that they had received an STR on the subject and the account had subsequently been closed.

4.1.2.3 Case Study 2: Fraudulent Wire Transfer through business enterprise scheme

Around May 2018, the FIA carried out an investigation relating to business enterprise scheme. In this scheme, financial institution X received an instruction through email allegedly coming from an employee of a corporate institution directing it to transfer about US$190,000 from the corporate institution's account to a service provider in foreign country Y. The instruction had all the necessary documents attached including service provider invoices. The email was purportedly from a corporate employee who is among those entrusted in processing and issuing payments. The transfer instruction had been duly signed by authorized signatories. Financial institution X processed and effected the transaction. However, after a week of effecting the transaction, the corporate institution queried financial institution X on the transaction indicating that it did not originate from them, meaning the letter of instruction was fraudulent.

After investigations it was established that the funds were fraudulently transferred to the alleged beneficiary in Country Y. It was also established that the funds had immediately been withdrawn from the beneficiary account.

The criminals are suspected to have hacked into the email of the employee of the corporate organization and used it to send instructions to the bank to make it appear as if it was sent by a trusted source when actually it was sent from a different account by a criminal.

Subsequent action

The FIA is still working with a fellow FIU in (Country Y) to trace the ultimate beneficiary of the stolen funds.

Indicators and Red flags:

- Instructions to make payments that appear legitimate and from expected official emails.
- Fraudster preferred bank account in jurisdiction where they believe the funds would be difficult to recover.
- Invoices, bank accounts and instructions to transfer the funds were sent from the email address that was almost identical to the legitimate email address of the customer.

- The funds were immediately withdrawn from the account leaving no trail of transactions.
- Instructions only done through email and not followed by telephone confirmation.
- Transactions involving large amounts of payments to other jurisdictions rather than within the country.

4.1.3 Typology 3: Money Laundering using alternative non-conventional methods

4.1.3.1 Introduction:

There has been a significant rise in transactions and movement of funds through the use of non-convectional payment methods that are paperless such as the internet, wireless devices (mobile/phone, point of sale machines), credit cards and debit cards. While commercial banks remain the core providers for these retail payment systems and services, payment platforms by other service providers in Malawi have similar electronic payment services and these include mobile phone service providers, merchants who have point of sale devices and money remitters like Mukuru, Hello Paisa, Zoona and Western Union.

This report has focused on the suspicious transactions and abuses of these non-conventional methods particularly Point of Sale machines, credit cards, mobile money, and electronic funds transfers. Individuals and financial institutions have been defrauded using these payment methods. The fraud cases involve a syndicate and conspiracy between the fraudsters of financial institutions.

Case Summary

Offence	Fraud, money laundering, obtaining money by false pretenses
Customer	Individual Customers, Merchants/Agents,
Products	Cash, Point of Sale Machines, Electronic Cards
Indicators and Red Flags	• Huge claims/credit balances of funds not commensurate with merchants' business and which do not make business sense • The urgency displayed by merchant to acquire the POS device • Transactions being done at odd hours • Transactions in the account only for settlement from the bank no other credits from other sources • Unusual credits made in the account • Suspicious/agitated third party presenting a cheque for immediate cash withdraw of large amount • Unusual transactions during the festive season or other holidays were people spend a lot of money

4.1.3.2 Case Study 1: Electronic Point of Sale Devices

A number of banks have introduced POS machines which are used by merchants who accept payments from their clients. The POS is a platform that allows people to purchase merchandise or pay for services using debit or credit cards. The merchants apply to the bank for the machines and are trained on how to operate them. After a transaction is done using POS, the merchants are refunded by the issuing bank the value of the transactions after 24 hrs.

The POS machines have capabilities of accepting cards from the issuing bank, other local banks and MasterCard from major financial institutions across the globe.

It has been noted that merchants in the tourism sector, particularly those operating hospitality establishments, are the major culprits in abusing the POS facility. MasterCard cards from other jurisdictions are the ones mostly targeted and used by conmen. Replicated cards are used for the scheme and huge sums of payments are made on the machines. The fraudulent transactions are usually identified when the POS issuing bank tries to get a settlement from the international financial institutions that own the MasterCards.

Within a period of 12 months, 2 banks have lost funds in excess of MK200 million and are still battling in court to recover the funds from both the merchants and the card issuers.

4.1.3.3 Case Study 2: Procuring Electronic Point of Sale Devices with intent to defraud banks and customers

In 2017 a merchant, Mr. Fisi (note the real name) operating a lodging business, opened a bank account with XYZ bank. The account was opened in the name of Wanga Enterprise (not the real name) and declared source of income and business was in the name of Zanga Lodge (not the real name). The same day the account was opened, a POS machine was issued and the first POS settlement was made on the account. This was unusual because it usually takes a minimum of 24 hours to have a transaction settled.

The account operated for a period of 2 months. The customer closed the account voluntarily citing poor customer care on the part of the bank. During the 2 months' period the customer had over 140 POS settlements done to the amount of K80 million (over US$100, 000)

Investigations later established that the client did not own or operate Zanga Lodge. The lodge though in existence is operated by different persons who allegedly are not aware of the POS machine and the transactions therefrom.

In 2018, the same client, Mr. Fisi, opened a bank account with bank ABC. He applied and was issued with a POS machine for his alleged business of selling different merchandise. Soon after receiving the POS machine, transactions and settlements were made.

Of interest is one particular day, 10 December 2018, when there were 28 transactions made on the machine, all of them were done at night after 22hrs. The transactions were from 10 cards and the sum totals of the transactions exceeded MK35 million (over US$45,000).

Upon discovery, the bank suspended the payments and did not honor the transactions. The bank further established that some of the cards used were also used on other POS machines within a space of less than 5 minutes, transacting over MK40 million (over US$50, 000). One card was used for transactions of over MK5 million (US$6, 000) on a mini-shop whose turnover is below MK1 million (below US$1,500).

4.1.3.4 Case study 3: Collusion between bank officials of the NPM providers and customers through the Electronic Payment systems

Bank JKL had trusted a well-known businessperson as one of its customers. Mr. Gwape (not his real name), the customer, operates a number of business accounts with the bank in which there are usually large cash transactions. He also has a personal account with the bank. History of the personal account shows that transactions in the account have always been below K1 million.

In December 2018, the customer, Mr. Gwape travelled to country D. On 24 December, Mr. Gwape contacted the bank informing them that he was having challenges with his Visa card which was linked to the personal bank account. When Mr. Gwape called the bank, his bank account balance was below MK100, 000 (i.e. below $150). The matter was referred to ICT personnel of the bank. Since the following 2 days were public holidays (Christmas and Boxing Day), the bank was not opened for business. When work resumed on 27 December 2018, it was established that the account was credited with about MK140 million (over US$190, 000) in three installments of MK100 million, MK20 million and MK20 million. By this day, over MK20 million had already been transferred out of the account through the visa card.

The matter was reported to FIA as a suspicious transaction report. The account was immediately frozen for preliminary inquiries. While the matter was being investigated, a third party presented a cheque to be cashed at one of the bank's branches. While the bank officials were consulting and doing background checks, the presenter of the cheque disappeared from the banking hall.

The bank established that the funds into Mr. Gwape's account was not his and was illegally transferred into the account by taking advantage of the holidays.

Furthermore, the matter was escalated and reported to the law enforcers. The person and the bank officials that were involved were arrested. The case is ongoing.

4.1.4 Typology 4: Financial Institution Frauds

4.1.4.1 Introduction:

In 2018, the FIA has observed that fraud has been a major threat to customers as well as financial institutions. This is in agreement to the results of the 2018 National Risk Assessment report which established that fraud is among the high-risk crimes that are yielding huge proceeds.

This report looks at the emerging trend that has been observed involving employees from banks who defraud customers through transfer of funds from customers' investments accounts and dormant accounts to their savings accounts.

Funds transfers are made from customers' accounts to fraudulent beneficiaries who in most instances are third parties (relations and friends of the employees). From the third party accounts the funds are transferred to the employees' accounts and later withdrawn. Thereafter cash is given to the employees. More importantly, there is a chain of funds transfers from one account to another to confuse the trail of fraudulent transactions and make it difficult for the banking system to detect the fraud. In addition, account details are changed, and accounts closed after funds transfers have been made.

It has been observed that employees of financial institutions in the remote service centers' target dormant accounts, especially those of customers who are residing abroad (for example, customers who have travelled and are working in South Africa). These individuals have used fake customer identity and forged customer's signatures to transact from the customer accounts. The employees have been syphoning funds through funds transfers from customer's account to their own nominated accounts. The unscrupulous employees also use forged cash withdrawal vouchers to cash from customer's account.

FIA observed that most of the accounts that have been targeted have easy-to-forge signatures. It is suspected the targeted clients are 'semi-literate' and just endorse their names as signatures. In some case though bank fraud can be done by third parties using fake IDs, cheque frauds.

It has been further established that other bank employees have taken advantage of KYC updating programs by providing phone number contacts for customers without the knowledge of the account holders to mobile money platforms. Once this is done, the accounts are connected to mobile phone payment platforms which enable them to transfer funds to other bank accounts and mobile money accounts. These observations have been made on inactive and dormant accounts and fixed accounts whose owners do not come forth timely to provide new instructions upon the maturity of the accounts.

Case Summary

Offence	Identity theft, Theft of cash, cheque book fraud, cheque fraud
Customer	Individual, sole proprietors, partnerships
Products	Withdrawals, cheque deposits, cheque encashment, Electronic funds transfer
Indicators	• Use of forged vouchers • Missing vouchers • Use of forged customer identities • Forging customer signatures • frequent changes of account details • Closure of accounts immediately after funds transfer instructions • Funds transfers involving multiple beneficiaries

4.1.4.2 Case study 1: Bank fraud from dormant accounts by Bank Officers

Mrs. Coins (not her real name) opened a bank account with bank UVW. She then left for South Africa. Cash deposits only were being made into the account while she was away by various individuals. The account accumulated funds amounting to MK15 million over a period of over 3 years with no withdrawals but deposits. Officer Mbuzi (not the real name), a teller working for the bank UVW, noted the trend in the account and effected withdrawals from the account on more than 3 occasions.

Officer Mbuzi connived with his supervisor, Mr. Finye, (not the real name) who was authorizing the withdrawals since they were above the transactional limits for teller Mr. Mbuzi.

Subsequently, the customer's inquiry on her bank account balance revealed that the balance was below MK60,000.00 which was far less than what Mrs. Coins had been depositing. Upon investigation, it was noted that millions of Kwachas were fraudulently cashed from Mrs. Coin's account by teller Mbuzi with the help of supervisor Finye. The cash withdrawal vouchers used were forged and some vouchers for other cash withdrawals were missing. In addition, the investigation revealed that 4 other bank officers were also stealing from customers' dormant accounts through funds transfers to different accounts as well as through cash withdrawals. The transfers to the different accounts were to third parties who later withdrew the cash on behalf of the perpetrators.

By the time the discoveries were made, teller Mbuzi was no longer with bank UVW as he had resigned. In addition, it was yet to be established as to the use of the cash withdrawn by the third parties on behalf of the perpetrators or themselves.

Furthermore, it was also established that lack of internal control checks contributed to the fraud. Moreover, checking of teller transactions were not done on daily basis as it is supposed to be the case.

Indicators and red flags

- Missing of transaction vouchers
- Forged customer signatures
- Use of forged customer identities and vouchers

4.1.4.3 Case study 2: Attempted bank fraud through a foreign cheque deposit

In June 2018, Company X deposited a foreign banker's cheque above US$ 1,000,000 in bank Y. In this case, bank Y was expected to confirm with the counterpart of international clearing as part of cheque clearing procedures. When the cheque was sent to international clearing house, it was discovered that it was a fraudulent cheque. As a result, the bank did not proceed with the transaction.

From the analysis conducted, it was revealed that the company has been transacting below MK 500,000 for close to 10 years and that no changes to income declarations were made to match such huge foreign cheque deposit into the account. In addition, it was discovered that the cheque was not cleared as it failed to meet the clearing procedures.

Subsequent action:

Further investigation into the matter

Indicators and red flags

- Huge amount of foreign cheques involving foreign banks.
- Cheque deposit amount not commensurate with customer's account activities

4.1.5 Typology 5: Insurance Fraud

4.1.5.1 Introduction:

Unlike the 2018 Trends and Typology Report in which disinvestment of insurance policies by clients was noted to be the main method for laundering of proceeds of crime from the insurance sector, the case is different in the 2019 Report. The FIA has identified cloning of cheques and online payments of pension benefits as an emerging method of laundering proceeds from the predicate offence of insurance fraud.

The FIA has observed that through these methods, funds are being stolen from the pension providers at point of payment of benefit within the value chain. The cloned cheques are exact replicas of the original drawn cheques down to the cheque number among other features. They are often created for the purpose of committing fraud. During the year, the FIA received 8 STRs from the insurance sector involving this method.

Case Summary:

Insurance related offence	N/A
Other offences	Insurance fraud, money laundering, theft,
Customer	Insurance company employees and individuals
Instruments methods and techniques	Pension and fraudulent payment to ghost beneficiary using cloned cheque
Indicators and red flags	• Legitimate beneficiary presenting the same (original) cheque to the bank • Presenters of cloned cheques pushing for quick processing of cheque • Insurance company respond that cheque was already confirmed • Receipt of pension which did not make sense • Amount of the monthly pension received • Bringing in of a third party who seems more in control than the client

4.1.5.2 Case study 1: Insurance employees defrauding the pension fund by cloning cheques

Around January 2019, the FIA carried out an investigation relating to pension payments by Insurance Company X on cheque number 700800 payable to Mr. Z amounting to MK11,500,000 through bank P. Mr. Z's account at Bank P was an illegitimate beneficiary. The account was created as a conduit to defraud Insurance Company X.

On 10 January 2019, an official of bank P, in their cheque processing, forwarded the cheque image to Insurance Company X for confirmation. The insurance company X confirmed the cheque.

On 11 January 2019, an official from another Bank M sent the same cheque image to the same insurance company X for confirmation. Upon receipt of the cheque image, the insurance company advised Bank M that the cheque was already confirmed and that the Bank should check with Bank P for possible duplication of the cheque. The second cheque was not processed.

Bank P confirmed that they already processed the cheque. It was established that the cheque that was presented to Bank P was cloned, whilst the cheque that was presented at Bank M was genuine. Bank P reversed the fraudulent transaction and later paid the funds to the legitimate beneficiary.

4.1.5.3 Case study 2: Theft of Pension funds through payments to ghost beneficiaries

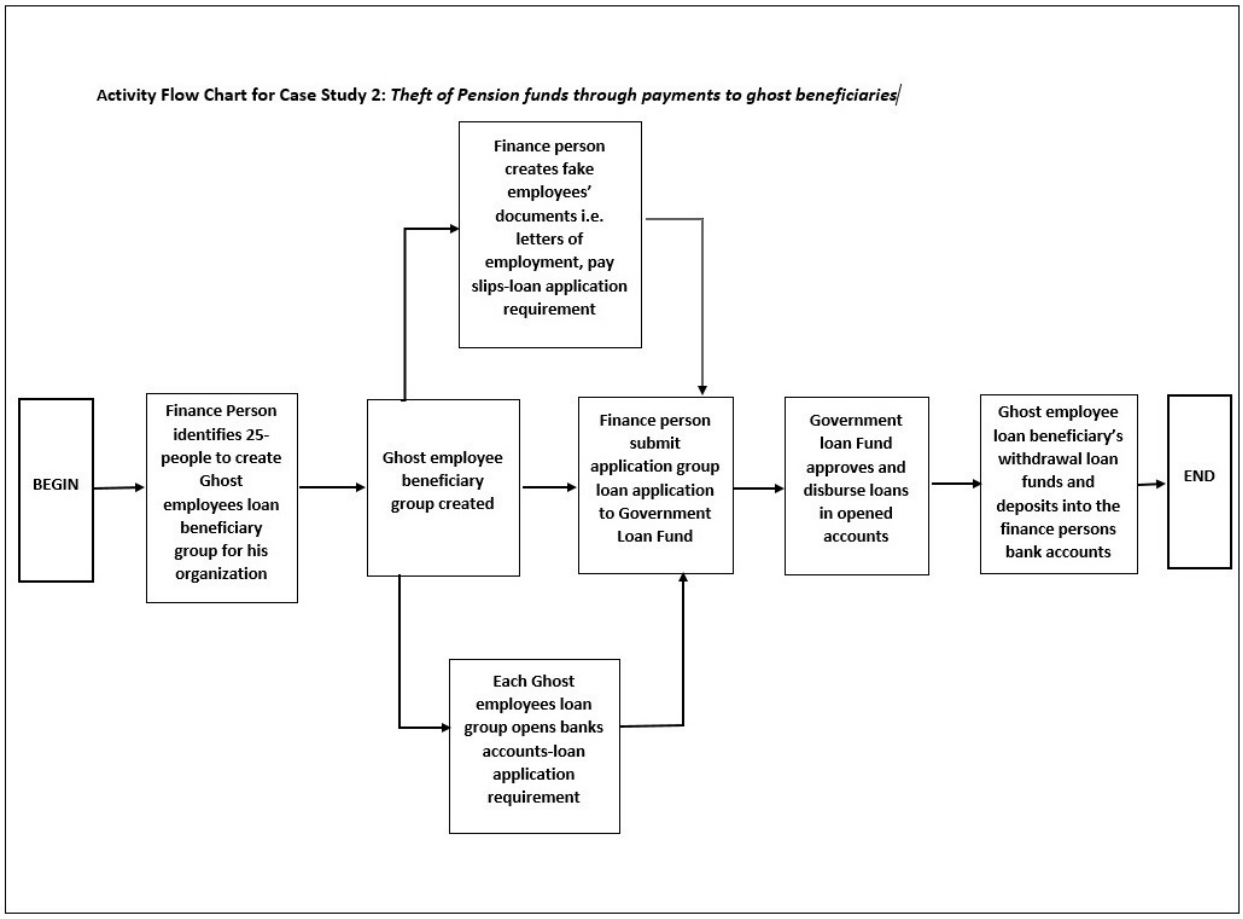
The FIA investigated a case in which person E has a business whose average monthly income is indicated as MK200,000. Person E maintained a personal account with Bank X. Further information indicated that person E is between 20 and 30 years old.

It was again established that person E's account also received a total of MK19,000,000 with monthly credits of around MK4,000,000. The funds were described as pension. However, this did not make sense because person E has not reached retirement age. Investigations established that the funds were paid by Insurance Company G and they were paid electronically into person E's account. These credits/deposits were followed by immediate cash withdrawals.

Bank X called the client for an interview on the source of the funds. The client showed up with an unknown third party who responded to most of the interview questions. It was later established through the insurance company that person E was not a legitimate pension beneficiary. It is suspected that the insurance company G's employees were involved. The account of person E at Bank X was created as a conduit to defraud insurance company G of the pension funds.

Subsequent action:

The case in on going.



4.1.6 Typology 6: Theft of Public Funds

4.1.6.1 Introduction:

In the period under review, FIA established a continuing trend of abuse and theft of public funds. However, there is a difference in the typologies used to pilfer public funds. Last year, the trend was observed in the payment of pensions, whilst this year the trend is in payment of salaries. Lack of checks and balances, for instance, laxity in transaction monitoring of the salary payments systems, provided some officers with an opportunity to tamper with the system. With this, they managed to insert higher amounts of salaries for themselves and other would be ghost public employees on the salary payroll, resulting in overpayment of salaries.

The payment system at the commercial banks created an opportunity for the unscrupulous officers to divert funds to accounts of the officers. A transaction is processed in the system on the basis of valid account numbers and not names. Therefore, as long as the account number is legit, a transaction is processed regardless of using fake/ghost account names. Furthermore, public Officials used third parties to receive and transfer the illegal proceeds and also concealed properties obtained from those proceeds of crime.

In the 2017/2018, there were interventions in which some of the perpetrators were arrested and the matter is still in court. The proceeds of the crime were confiscated. However, despite the intervention, the trend is seen to be continuing.

Case Summary

Offences	Money Laundering, theft by public officer, conspiracy to defraud, impersonation, uttering false documents, obtaining money by false pretense.
Customer	Public Officer, Individual
Instruments methods and techniques	Transfers and payment instructions, Bank accounts, fictitious application, loans,
Indicators and red flags	• Irregular huge amounts of salary credits • Deposits followed by immediate cash withdrawals • Third parties • Several individual accounts channelling huge sums to three individual accounts

4.1.6.2 Case study 1: Theft of Public funds through overpayment of salary

FIA investigated a case in which person A working in the Public Service has an estimated net salary of MK70,000. However, person A's account had been receiving funds described as Malawi Government salary. Person A was crediting his own account with these funds. Between April 2017 and November 2018, person A credited his account with a total amount of MK60,500,000.

4.1.6.3 Case study 2: Abuse of Government Loan fund through creation of ghost beneficiaries

FIA worked on a case where finance officer K of Organization B created a beneficiary group of about 25 people disguised as employees of Organization B to benefit from a Malawi Government loan revolving fund. Employee K colluded with a public official from a Government Loan Facility who facilitated for the group members to receive various amounts of loan. The total amount of loan that the group received was about MK90,000,000. The finance officer K created documents such as letters of employment and pay slips required in application of the loan as if the 25 people in the group were employees of organisation B while none was employed except himself. He forged signatures and documents as part of the process.

When the loan funds were credited to each of the group members' bank accounts, finance officer K instructed all the group members to withdrawal the funds and deposit into his personal and business account. Though the finance officer eventually received the loan funds from the group members, he did not start to pay back the loan.

It was also established that the group members were not aware that the funds were from Malawi Government loan revolving fund. Finance officer K informed the group members that the funds were loan from his employer.

Subsequent action:

- Investigation
- Arrests made
- Recovery of some of the funds

5 PART E: RECOMMENDATIONS

RECOMMENDATIONS

This section outlines recommendations for various stakeholders to implement with the aim of preventing, detecting, investigating, prosecuting and following the proceeds of money laundering, terrorist financing and other financial crimes. The ultimate goal is to prevent criminals from enjoying proceeds of crime through confiscation and forfeiture.

5.1 Improved control environment

It has been noted that most of the fraud in both public and private entities are made possible due to lapses in internal controls. One of the lapses is collusion between officials and third parties. Therefore, we recommend that entities should review the internal controls and ensure that fraud of any kind is prevented, if not, detected. For example, there should be some face-to-face verification of public loan beneficiaries before disbursing funds to individuals. This will ensure disbursement of funds to legitimate beneficiaries. Regarding government entities, the government payment systems should introduce more checks and balances that will leave audit trails for easy follow up of personnel's misconduct.

Financial institutions should continue to verify payments instructions through appropriate channels in order to prevent BEC, cheque and other types of fraud. These may include verification through Person Identification Number (PIN) and telephone confirmation. In addition, these entities should conduct awareness programmes to sensitise their customers and staff on the possible frauds that may be targeted towards them.

5.2 Enhanced KYC exercise and vetting of employees in banks

Since some types of fraud are facilitated due to lack of customer and staff screening. Regarding customer screening, financial institutions should ensure that additional particulars are collected from applicants of bank accounts. The suggestions include taking of fingerprints and photographs for customers. They should also consider using standard identification such as the national identity card that can further be corroborated with the National Registration Bureau (NRB). As regards staff screening, banks should ensure that necessary procedures are followed when employing staff such as staff vetting.

5.3 ML/TF awareness

There should be continued implementation of policies and codes of conduct in public entities. Apart from theft, the codes of conduct should include suspicion of money laundering as a case warranting disciplinary hearing and dismissal. Employees should be made aware of actions that would be equal to committing money laundering. These actions include; converting, transferring, concealing, disguising, acquiring,

possessing and using property from proceeds of predicate offence as provided in section 42 of the Financial Crimes Act (FCA), 2017.

5.4 Improved ML/TF investigations

LEAs should introduce standard operation procedures (SOP's) for investigating crimes to do with public loans/funds theft. Future investigations should include methodologies to identify and investigate money laundering offences.

Government agencies and banks should collaboratively conduct regular exercises on harmonizing bank account holder particulars to be undertaken by both government agencies and banks in collaboration.