FINANCIAL INTELLIGENCE AUTHORITY

With a vision for a financial crime-free Malawi

MONEY LAUNDERING TRENDS AND TYPOLOGIES REPORT 2019-2020

Contents

PART A: GENERAL INFORMATION

1.1 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

1.2 ACRONYMS AND ABBREVIATIONS

Abbreviation	Definition
AML/CFT	Anti-Money Laundering/ Combating the Financing of Terrorism
CDD	Customer Due Diligence
DNFBP	Designated Non-Financial Business and Profession
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	Money Laundering
MVTS	Money and Value Transfer Services
NPM	New Payment Methods
STR	Suspicious Transaction Report
TF	Terrorist Financing

1.3 INTRODUCTION

The cost of financial crimes to countries continues to be felt and this has seen governments accelerate efforts in the fight against these vices. As the world continues to witness the incorporation of proactive methods alongside the record reactive methods to fighting financial crimes, access to information plays a vital role. Right information empowers law enforcement agencies (LEAs), various stakeholders and the public with necessary tools to inform their proactive strategies to fight financial crime.

Advancement in technology has enabled an enhancement in deterring methods on the part of those entrusted with fighting financial crime. However, criminals are equally capitalizing on the same advancement and are driven even further to inventing new ways to commit crime. The Financial Intelligence Authority (FIA) recognizes the important role that access to the right information plays in strengthening Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) regime thereby contributing towards the vision for a financial crime free Malawi.

Mindful of this shift towards proactive strategies to fighting financial crime, the FIA is confident that the dissemination of strategic intelligence to LEAs and other relevant stakeholders will provide them with an enabling platform to make informed proactive countering strategies to halt financial criminals in their tracks, or disrupt financial crime syndicates way before they strike, among others.

This Trends and Typologies Report is one way the FIA continues to reach out to stakeholders with intelligence which informs them on the best practices as well as acting as a source of knowledge on ML/TF and other financial crimes. The report sets out to strengthen the various stakeholders in their efforts to countering financial crimes including money laundering, terrorist financing, bribery, corruption and fraud through various methods.

As LEAs and various stakeholders access this report, the FIA is confident that it will continue to inform them of the various financial crimes, and in turn the information will apprise their proactive strategies to fighting financial crimes. Consequently, the report will contribute to reduction in financial crimes and enhancement of the integrity of the country's financial system. This will ultimately lead to a realization of tangible growth in the economy.

1.4 EXECUTIVE SUMMARY

FIA's 2019/2020 Trends and Typologies report illustrates a number of areas that include new and emerging trends used by criminals to gain illicit proceeds. The new and emerging trends include Money or Value Transfer Services among others. In addition to this developing trend, others which continue manifesting include International Funds Transfers disguised as insurance premiums for falsified loans; use of Prepaid Express Card; use of improved payment methods such as Prepaid Cards and Mobile Money. The year has also witnessed the re-surfacing of use of false documents.

It is significant and worth mentioning, the new trend which involves ML through use of Money or Value Transfer Services (MVTS). MVTS refers to;

> financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. [1]

The acceptance is done in one location and payment of a corresponding amount in cash or other form to a beneficiary is done in another location. Examples of MVTS include dealers in foreign exchange; cheque casher; issuer of traveler's cheque or money orders; money transmitter; and provider and seller of prepaid access, payday lending and bill payments. MVTS operators are licensed and registered services which operate through agents or a network of agents.

Criminals carrying out Money Laundering and Terrorist Financing are taking advantage of the MVTS owing to its quick and cash-based nature. Unlike banks, for instance, MVTS operators rarely generate long term relationships with their clients. This renders suspicious activities through MVTS to be difficult to detect through ongoing monitoring. Therefore, criminals capitalize on these shortcomings of the MVTS and have recently engaged in frequent use of these services to launder illicit proceeds. It is therefore important for agents of MVTS to be vigilant in noting the red flags that are associated with the use of MVTS such as sudden increase in outward or inward funds for individual clients.

In promoting furtherance of access to information, and in line with its core functions, the FIA is confident that it is vital that the LEAs, the general public and other stakeholders are kept abreast of how criminals are now increasingly adopting MVTS as a discreet way to launder proceeds of crime. This will help users

[1] www.fatf-gafi.org

of this report to make informed and efficient proactive strategies to deterring ML through the MVTS.

The report also highlights some continuing trends such International Funds Transfers with instructions or guidance from multiple customers or third parties; use of Prepaid Express Cards; Theft of Public Funds; Financial Institution Fraud and use of New Payments Methods (NPM) such as mobile money payments and prepaid cards. In the previous report, the theft of public funds manifested itself through bogus payment of salaries and pensions. The trend in the year under review has been paying out money to beneficiaries or suppliers without the required supporting documents. This trend has created a platform where senior officers in government are seen to abuse their junior officers by engaging them to process the payments without following government's laid down procedures. Other senior officers have been observed to disregard their role in observing procedures by simply authorizing payments by overriding controls. The government, as a result, has in the year under review lost significant amounts of money through such override of controls by senior management who are essentially supposed to be custodians of government procedures and internal controls.

Financial Institution fraud has also been seen to flourish in the reviewed period. This kind of fraud is committed against the financial institution by its own officers. They do this by abusing their positions for personal gain. Employees of Financial Institutions are aware of their own systems' weaknesses and capitalize on that to sometimes coordinate with third parties to defraud suspense and customers' accounts.

It is of significant interest to note how the novel corona virus pandemic may have exacerbated the use of New Payment Methods as a means to defraud individuals. The economic strains that the pandemic has brought with it has left people jumping at every seemingly promising opportunity to earn money. Criminals have capitalized on the current economic situation and have managed to defraud people through empty promises of financial helping hand or support. The most frequent used method is where criminals use mobile numbers through Short Message Service (SMS)'s or voice calls to lure unsuspecting individuals into submitting personal information to the criminals and in the end getting defrauded.

Another method that has been observed continually is the use of Subscriber Identification Module (SIM) card swapping. Since both the agents and recipient of mobile money make use of electronic wallets which are connected to their mobile numbers, it requires authentication which usually is a text message. Criminals have taken advantage of such a system and manipulated text messages to unsuspecting individuals to make them seem authentic and consequently defraud people of their money.

The report also touches on the use of false documents, which is a trend that has re-surfaced and continues to be employed in the operations of criminals of ML. Utilization of falsified cheques and identification as well as opening and operating bank accounts using falsified documents are the notable ways that financial criminals have continued to employ.

PART B: OVERVIEW OF SUSPICIOUS TRANSACTION REPORTS (STRs) RECEIVED

1.5 General observations from STRs and Financial Investigations

This section provides a general overview of the Suspicious Transaction Reports (STRs), which the FIA received from reporting entities and subsequently analyzed. It also provides details on financial investigations conducted and financial intelligence disseminated to Law Enforcement Agencies (LEAs) and other relevant stakeholders.

STRs are a vital source of information in identifying funds that may have been used for criminal activities including money laundering and terrorism. As a result of the analysis and financial investigations of these STRs, criminal patterns and trends were identified. These are identified together with the ML/TF vulnerabilities and indicators of such techniques or methods. This information is important for both FIA, reporting entities, law enforcement agencies, regulatory bodies, and supervisory bodies.

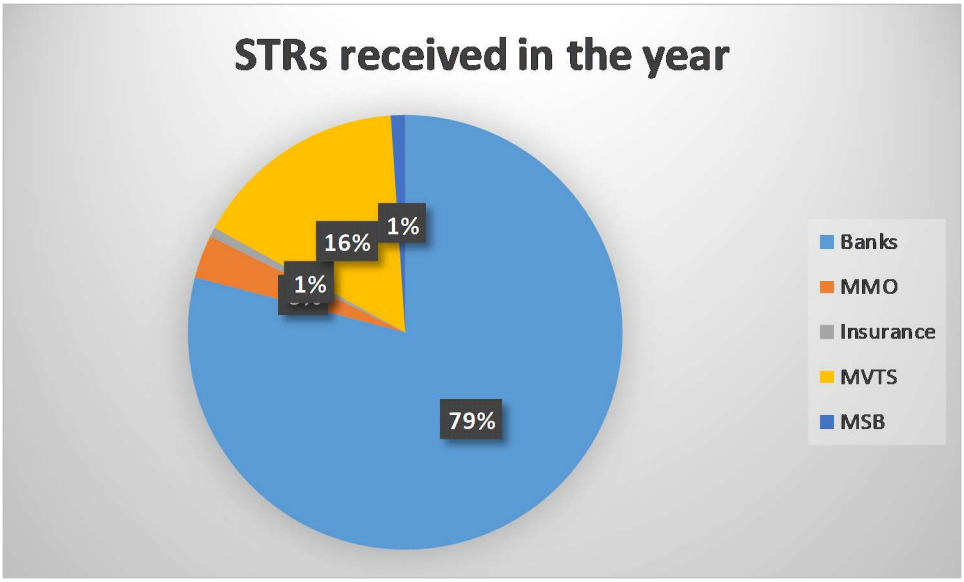
These indicators will significantly assist the financial institutions and other accountable or reporting institutions in developing an effective AML/CFT regime. A good AML/CFT regime is vital for preventing individuals and criminal organizations from using financial institutions to launder proceeds derived from crimes thereby maintaining the integrity of the financial system. In addition, 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 analyzed from the various reporting entities for the fiscal year July 2019 to June 2020. During this period, a total of 16 reporting entities filed STRs with the FIA. The total number of STRs was **282**. The banks submitted **223** of the STRs representing **79%**. The remaining **59** were from the insurance sector, Mobile Money Operators (MMOs), MVTS Operators and Money Service Businesses (MSB). There was no STR filed with the FIA by Designated Non-Financial Businesses and Professions (DNFBPs).
- Requests for information from law enforcement agencies.
- Media reports and other open sources information.
- Information available to the FIA from other Financial Intelligence Units (FIUs) or similar institutions in AML/CFT.

Pie chart 1 below presents summary statistics of STRs received by FIA from the reporting institutions by sector. What stands out in the chart is that the traditional Financial Institutions sector is leading in reporting STRs compared to the other sectors.

Pie chart 1: STRs received for the year per reporting sectors



1.6 Common / Prevalent Indicators observed

Below are some of the most prevalent techniques and indicators in the STRs received by the FIA;

- Business account receiving huge amount of funds transfers inconsistent with the business profiles. The funds are subsequently transferred into other bank accounts or withdrawn from the account within a short period of time.

- Transactions which are inconsistent with customer profile. The transactions do not match the declared source of funds, income or status, or business activity.

- Customer regularly receiving funds from multiple sources followed by immediate withdrawals, usually in a different location. These are mostly personal accounts which have no indications that the holder is engaged in any business.

- 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 transfers large amounts of foreign exchange to foreign jurisdictions.

  Tax evasion through structuring of import payment so that each importation is below the limit for customs duty. This is done when a businessperson imports a large consignment of goods but paid and received as multiple small parcels.
- 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 account holder.

- Customer requesting to change beneficiary other than the one on the import documents. Whereby the requested destination of funds not matching the jurisdiction and source of goods imported.

- High levels of cash deposits in excess of expected legitimate banking activity of the account holder.

- Multiple international funds transfers sent to the same beneficiary. Companies with different types of business importing and making payments to a common beneficiary.

- Multiple third-party cash deposits into the same account followed up by outward international transfers.

- Social engineering scams for mobile money. This is done when fraudsters dupe their victims into disclosing confidential information thereby hacking the victims account. Also, when fraudsters send fake messages to their victims, enticing them to send money to the fraudster by using psychological manipulation e.g. money to rescue a stranded relation or money to claim a prize. A similar to this is phishing where a fraudster tricks unsuspecting people into giving information over the internet or by email in order to take money from them.

- Identity theft and Subscriber Identification Module (SIM) card swap. This is when fraudsters manage to change and register a new sim card of a victim. Once the swap is done the SIM card that the victim uses is rendered useless and there is an automatic transfer of mobile wallet account from the victims' phone to the fraudster's SIM card.

- Impersonation of service providers by fraudsters. Victims receive messages purported from service providers advising or instructing them to update

their information. In the process, the customer's Personal Identification Number (PIN) code is compromised.

- Dubious requests for refund for money purported to have been sent to a wrong account.

- Frequent and multiple loading of cash for mobile money that do not make business sense based on customer profile and business returns.

- 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.

- 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.

- An increase in incoming funds activity for an individual with no history of such activity or where the stated customer business has inconsistencies.

- Dormant account suddenly receive incoming transfers followed by immediate withdraws

PART C: MONEY LAUNDERING AND TERRORIST FINANCING METHODS AND TECHNIQUES

This section aims to delineate the noted trends into different categories. The trends have been classified in terms of continuing, emerging and prevalent money laundering methods and techniques. Notably, criminals continue to take advantage of the vulnerable sectors in the financial sector to commit financial crimes and launder the proceeds generated. It has been generally noted that money laundering activities are moving to other non-financial sectors especially with the use of New Payment Methods (NPM) such as electronic money.

With respect to continuing trends, it is believed that the public sector remains one of the most vulnerable sectors in Malawi. This is because there has been a continuing trend in a way that Government employees continue to take advantage of the loopholes to steal public funds. They abuse their powers by putting aside government laid down procedures and controls. It has further been noted that the proceeds are laundered through real estate and investing in legitimate businesses. Apart from these methods, funds are also believed to be laundered through creation of third party businesses and ghost workers whose bank accounts are used to receive the stolen funds. Later, the stolen funds are moved and invested in real estate and purchase of luxury goods. On the other hand, it can be said that the efficient KYC and due diligence measures being enforced by some reporting entities has led to the detection and hence their reporting to the FIA.

Another continuing trend is money laundering through exchange control violations. In addition to the traditional methods and Trade Based Money Laundering (TBML) methods, the Authority also noted that some criminals resorted to the creation of bogus investment schemes. For instance, criminals employed third party companies who disguised themselves as investors. The investors created a scheme in partnership with offshore companies. In turn, the offshore companies were acting as major financiers through loans to these local investors. However, the offshore companies deceptively demanded insurance premiums and management fees from the local investors. In that way, the local investors had reasons to legitimately move funds to offshore accounts disguised as insurance premiums and management fees.

The volumes of the funds moved were in millions of United States Dollars (USD). It was further noted that the purported loan funds had never been provided to the local investors despite the huge amount of funds that were sent to the offshore accounts to finance these loans. Once the payment made successfully, the

transaction stalls without any funds in form of loans or grant wired in to the financial institution. Suspiciously, the local investors (financial intermediary) received small amounts of funds from offshore businesses for the purpose of salaries and setting up of offices. However, the FIA suspected that the funds received by the local investors were likely commission for facilitating the movement of the funds to the offshore accounts.

As far as emerging trend is concerned, the money laundering through use of New Payment Methods mainly involved the transfer of proceeds through use of stored value. Currently, there is a significant push by the Financial Regulators for people to use electronic transactions. Financial institution customers who use electronic payments generally use traditional money to purchase e-money from service providers and then use the stored value to buy goods and services from merchants. However, due to the lower threshold amount in the use of electronic payments such as mobile money, users tend to have multiple accounts which they use to move significant amounts of funds across the borders. In addition, scammers have also utilized the NPMs to defraud people because of the anonymity associated with the methods. Electronic methods are fast and do facilitate movement of funds without intervention of the financial institutions.

Regarding prevalent trends, the FIA noted money laundering activities through the use of false documents in financial institutions. The false documents were used to open accounts with an intention of conducting fraudulent transactions. The criminals used the accounts opened using false documents to clear forged cheques. The section that follows discusses these trends through case examples and highlights the noted red flags or indicators.

PART D: MONEY LAUNDERING TRENDS AND TYPOLOGIES IN MALAWI

1.7 CONTINUING TRENDS

1.7.1 Typology 1: Theft of Public Funds

Introduction

In the period under review, FIA established a continuing trend of abuse and theft of public funds. Last year, the trend was observed in the payment of pensions and salaries, whilst in this year the trend is in payments to beneficiaries/suppliers without supporting documents from government. It was observed that senior officers exercised dominance over junior officers who were instructed to process payments without following Government laid-down procedures and internal controls. In addition, some senior officers abandoned their responsibility as custodians of internal controls thereby authorizing payments without due regard to set procedures.

In this trend, it was observed that government continues to lose significant amount of funds due to senior officers' abandonment of responsibility to ensure adherence to government procedures and internal controls. For example, government payments were done by overriding well implemented controls such as validation of supporting documents or payment instructions. for A typical example in the 2019/2020 financial period, Malawi Government lost over MK350 million through payments to a single beneficiary.

These senior public officials created private businesses registered in the name of third parties, often relatives or girlfriends. However, the officials still maintained control of the funds through new technologies of conducting transactions offered by the financial institutions such as mobile banking. Through such platforms, the funds were moved to their accounts where they were later invested in real estates, motor vehicles and also in maintaining luxury life styles for themselves and their relatives or girlfriends.

In the previous year, the FIA detected some businesses which received Government funds without offering any service. Through the intervention of FIA and MPS, some of the perpetrators were arrested and their cases are still in court. Some stolen funds were traced, frozen and preserved. Apart from the funds, other assets such as real estates and motor vehicles derived from proceeds of the crime were traced and restrained in order to be used to satisfy a pecuniary penalty order.

1.7.1.1 Case study: Theft of Malawi Government funds by Senior Public Official through fictitious payments

Case Summary

Offences	Theft by public officer, Money Laundering.
Customer	Business and individual
Instruments, methods and techniques	Transfers, mobile banking, bank account, cash withdrawals
Indicators	Business account receiving huge amounts of funds transfers inconsistent with the business profiles. Deposits followed by transfers to the personal account. Account transactions inconsistent with customer profile. Preferential use of mobile banking to transfer funds through mobile banking by targeting daily limits. Use of third party accounts in an attempt to make the transactions look legitimate

Case description

FIA investigated a case of a senior public official working in the public service as a Manager. The official, who was responsible for authorizing transfers of government funds to beneficiaries, abused his powers by authorizing payments without validation of the supporting government instructions. The senior public official took advantage of the junior officers by instructing them to capture huge amounts into the system without supporting documents. The captured amounts were in favour of beneficiaries who did not provide any service to Government. The major beneficiary was a business registered by the girlfriend to the senior public official and the other beneficiaries were also significant others. Through the created scheme the official stole more than MK350 million over a period of 12 months.

Brief details of the payments are that firstly a business registered by Girlfriend A received 9 payments amounting to over MK340 million from Government authorized by the senior public official. Following this, the Girlfriend registered the mobile number of the senior public official on the mobile banking platform so that he could be in control of the funds himself. Through this platform, the senior public official was able to transfer the funds from the business account into his personal account and later withdrew the funds to develop real estates, procure motor vehicles and support other girlfriends.

Secondly, Girlfriend A received additional 2 payments in her personal account amounting to over MK10 million from Government without providing any service. The funds were authorized by the same senior public official.

Finally, Girlfriend B of the senior public official received 1 payment authorized by himself. The funds were used to procure a motor vehicle at the instruction of the senior public official.

Subsequent action

- Arrests
- Freezing
- Restraining
- Preservation

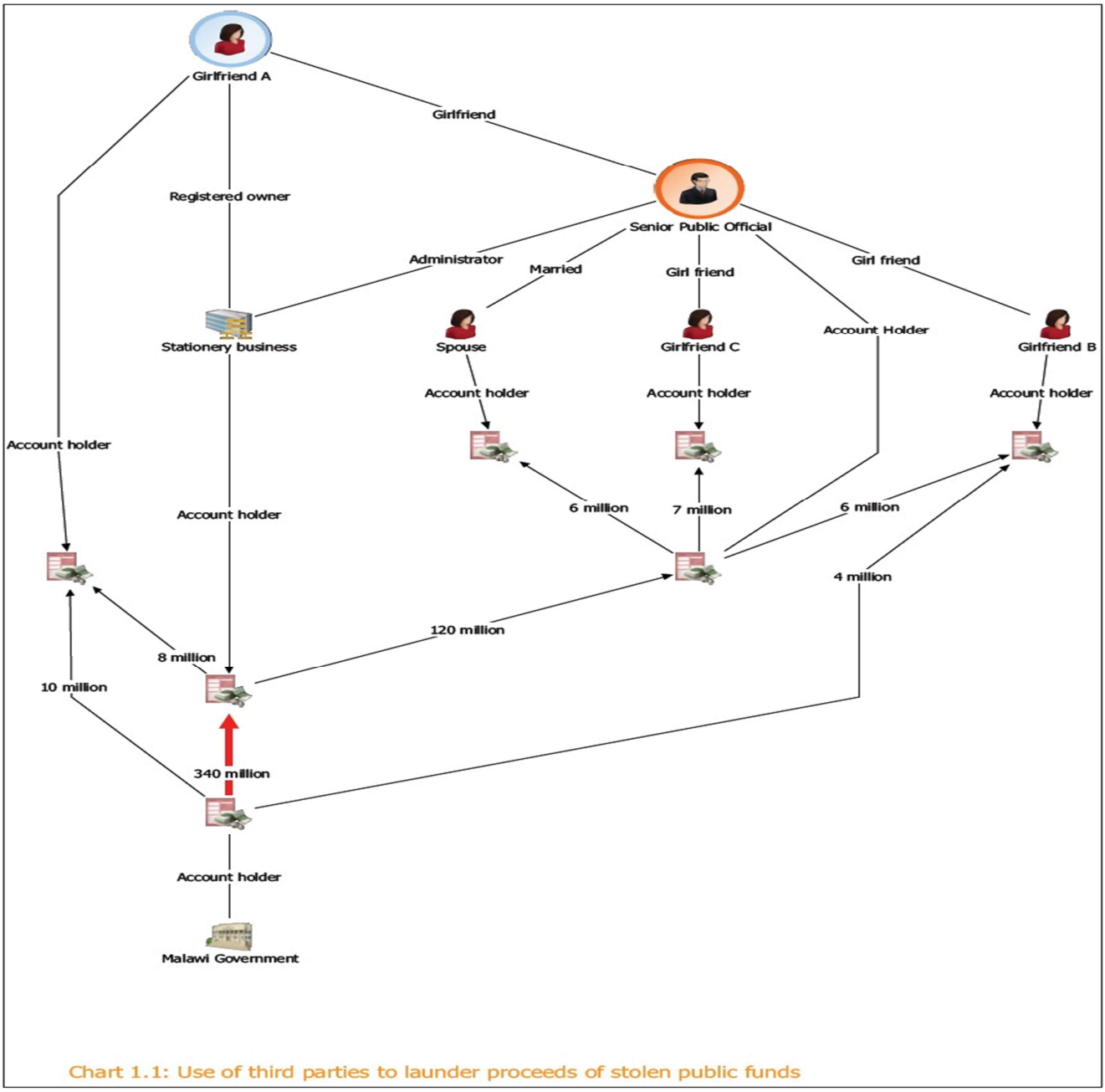


Chart 1.1: Use of third parties to launder proceeds of stolen public funds

1.7.1.2 Case study: Payment of salaries to ghost workers

Introduction

As indicated earlier, the FIA established the continued trend of theft of public funds through ghost workers. The perpetrators opened bank accounts which were later used to receive payments with transaction description of payroll from various Government ministries and departments. The FIA analysed the bank accounts and noted that they were opened during the same period and had the

same transaction dates and amounts. The accounts were funded twice only with funds from Government. The accounts were abandoned after withdrawing the funds. Notably, a substantial number of the analysed bank accounts belonged to women.

Case summary

Offences	Theft, money laundering.
Customer	Individual
Instruments, methods and techniques	Transfers and payments, bank account, cash withdrawals
Indicators	Dormant accounts. Different sources of funds from what was declared. Use of false information. Huge amounts not matching the declared amount.

Case description

Mrs. Gogo (not real name), is a business lady involved in buying and selling of maize. She declared her monthly income as MK30,000 from this business when opening her account with Bank D. The account was opened in May 2019. In the course of the business relationship, Mrs. Gogo received MK1,500,000.00 in June 2019 and MK2,500,000.00 in August 2019 in her account. The funds received in Mrs. Gogo's account were from Department Y of Government. The description for the transaction was specified as "payroll". It was noted that these were the only credits into the account described as payroll for a period between 24th May 2017 and 24th August 2019.

What stood out with her account was the lack of consistency of payroll amounts being credited into her account. Furthermore, it was established that Mrs. Gogo was not a Department Y employee. The findings established that Mrs. Gogo was a ghost worker.

Subsequent action

- Investigation
- Name removed from payroll list
- Closing of bank account by Bank D

1.7.1.3 Laundering proceeds of crime through Real Estate.

Introduction

During the financial year 2019/2020 the FIA noted that some businesses and individuals were using the real estate sector to reinvest stolen funds. The sector is vulnerable as it attracts an investment opportunity to further grow the money. It should be noted that the National Risk Assessment of 2018 established the Real Estate sector as posing the highest risk for money laundering in Malawi. Additionally, investing of proceeds of crime through real estate is becoming an established method of money laundering. The most commonly identified methods that criminals use to launder funds into the real estate sector include:

- Purchasing of real estate using cash.
- Use of illicit funds to pay for renovation in order to increase its value.
- Buying or constructing real estate using a third party or family member as the legal owner.
- Property is either purchased on their behalf, or proceeds of crime are deposited into their bank account to conceal the purchase.
- Use of large volumes of cash to buy property involving legal practitioners.

1.7.1.4 Case Study: Bank fraud and laundering the proceeds into Real Estate

Case Summary

Offences	Fraud, money laundering
Customer	Individual, bank, shell company
Instruments, methods and techniques	Wire transfers, ATM and over the counter withdrawals
Indicators	Transferring funds from suspense accounts. Stealing the funds from the bank vault. Transferring the funds to nominees.

Case description

Mr. X, was a senior manager at a local bank. Through his dealings with a third party, he siphoned the Malawi Government significant amount of money through

creation of false payments to beneficiaries. His position in the bank allowed him to process and authorize government payments without raising suspicion.

Through his collusion with a third person, they both registered a shell company which he later used to siphon the public funds from. The third person would periodically withdraw the money and hand it over to Mr. X. It was revealed during investigations that a substantial amount of the funds was used to buy plots of land, construct houses and make improvements to some of the properties.

Subsequent Action:

- Arrests
- Charges of theft and money laundering
- Seizure
- Forfeiture

1.7.2 Typology 2: International funds transfers with instructions or guidance from multiple customers or third parties.

Introduction

Another continuing typology is on foreign currency control violation. In the period 2019/2020, the FIA uncovered a scheme in which some companies illegally externalized funds to offshore accounts using a company. This may be categorized as use of third party. The company followed the legal means by obtaining the necessary authority to send the funds outside the country. During the period under review, the funds were remitted through 3 financial institutions. It was further noted that the funds were remitted as contribution to a credit facility and insurance premium in respect of a prospective loan facility.

1.7.2.1 Case study 2.1: Exchange control violations through remittance of insurance premium and management fees for falsified foreign loan

Case Summary

Offences	Illegal externalisation of forex and money laundering
Customer	Individual, company
Instruments, methods and techniques	Bank accounts, loans, remittances
Indicators	Huge value of international funds transfers to European beneficiaries. Multiple huge international transfers sent by same Company to multiple beneficiaries in Europe. Receipt of funds from a business in Europe by remitting company in Malawi

Case description

In 2019/2020, the FIA worked on a case where Company A requested for authority from the Central Bank to remit huge amount of funds to some beneficiaries in Europe on behalf of some companies in Malawi. The application stated that the remittances were in respect of an establishment of a standby letter of credit, management fees and advance insurance premium in respect of prospective loan facility. The remittances were done through 3 financial institutions as follows;

In Financial Institution A, Company A requested to remit over Euros 700,000 (MK578.9 million) to a beneficiary in Europe. The funds were insurance fees for a loan of over Euros 9 million (MK7.4 billion) which Company A secured from the beneficiary in Europe.

In Financial Institution B, Company A requested to remit over GBP445, 000 (MK402.7 million[2]) to a beneficiary in Europe. The funds were insurance premium, management fees, and notary and stamp fees for a loan of over Euros 6 million (MK4.9 billion) from the beneficiary.

In Financial Institution C, Company A requested to remit over GBP2 million (MK1.8 billion) to a beneficiary in Europe. The funds were facilitation fees for a loan agreement of over USD15 million (MK11 billion) from the beneficiary.

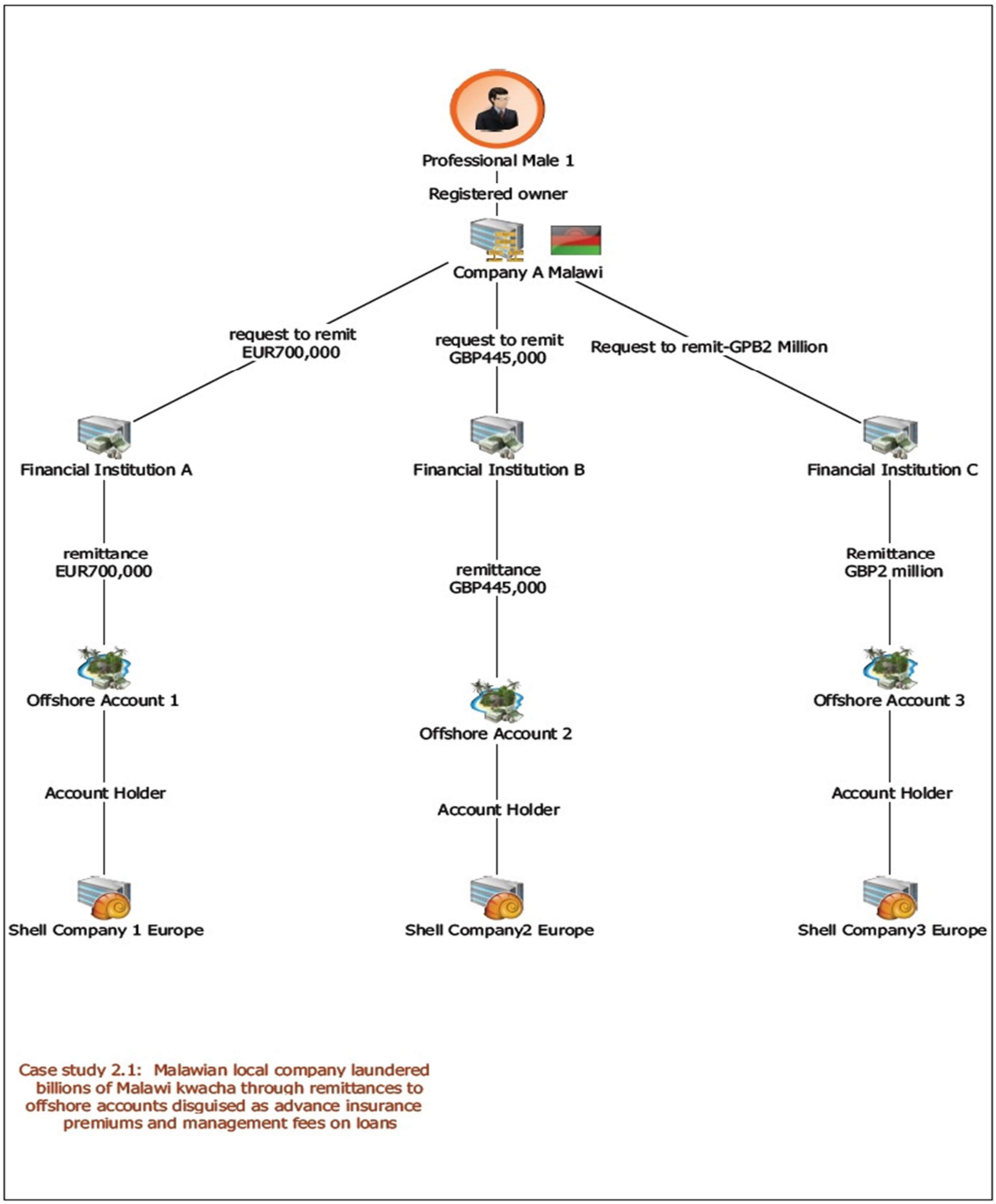
Although Company A provided a timeframe in which the loans would be disbursed to Malawi, none of the funds ever came to Malawi upon expiry of the agreed timeframes. Instead, Company A kept on shifting the timeframes.

[2] Reserve Bank of Malawi (RBM) middle rates as at 30 June 2020

However, whilst waiting for the funds, Company A received over USD15,000 (MK11 million) from Europe. The funds came from a related party to the company that was beneficiary of the funds purported to be insurance premium and management feed. Company A stated that the funds were in preparation for receipt of funds and also for organizing their office. However, it was suspected that the funds were commission for illegally facilitating remittance of funds to Europe.

Subsequent action

- Freezing of funds
- Revocation of authority to remit funds



Case study 2.1: Malawian local company laundered billions of Malawi kwacha through remittances to offshore accounts disguised as advance insurance premiums and management fees on loans

1.7.2.2 Case study: Exchange control violations by a business which altered beneficiaries on the Import payment documents

Case Summary

Offences	Illegal externalisation of forex and money laundering
Customer	Business
Instruments, methods and techniques	Bank accounts, remittances
Indicators	Customer requesting to change beneficiary name other than the one on the import documents. High levels of cash deposits in excess of expected legitimate banking activity of the account holder. Multiple international funds transfers sent to the same beneficiary. Multiple third-party cash deposits into the same account followed by outward international transfers.

Case description

In another case regarding exchange control violations, the FIA worked on 8 cases where businesses made huge import payments beyond the expected transaction activity of the businesses or account holder. The import payments were over MK6 billion over a period of 10 months across three financial institutions. The bank accounts received multiple huge cash deposits by third parties which were followed by outward international transfers as import payments. These transfers were done to the same beneficiaries. Some businesses attempted to change beneficiaries from the one on the import payments. On the other hand, for some businesses the account holder could not furnish the required information of the transactions taking place in their accounts. Besides, some business locations could not be traced, thus bringing suspicions that they might either have closed after making the transfers or they did not exist at all.

For instance, Business entity A made import payments amounting to over USD1.7 million (MK1.2 billion) in just 2 months to 2 beneficiaries. The business is involved in

manufacturing low cost plastic shoes. The invoices supporting the import payments showed that the business was importing various machines. There were frequent huge cash deposits by third parties into the account which were followed by outward international transfers. It is suspected that several individuals could have been using the business account to externalize funds under the disguise of import payments. The account holder also made attempts to change the beneficiary of the funds from the one on the invoice supporting the import payments.

It was further noted that business entities B and C were registered by the same person. The two businesses in total made import payments amounting to over USD1.2 million (MK884.4 million) in just 10 months to a single beneficiary. The businesses are involved in the selling of salt and groceries. However, the transactions with the accounts did not make business sense. Firstly, the business annual turnover declared was about MK10 million, but managed to import amounts that were more than the declared income without any explanation for the difference. Secondly, the transactions in the period were not consistent with the customer profile. Thirdly, the account holder was not able to explain the transactions in the account. Further, the business location indicated in the account mandates could not be traced and all the contacts could not be reached. It is highly likely that the business was a front business used to externalize funds disguised as import payments.

In the case of business entities E, F, G, H and I, they were all involved in the selling of general merchandise. It was noted that the declared annual turnover of the businesses was not commensurate with the customer profiles. Moreover, the transaction pattern was mainly huge cash deposits by multiple individuals followed by outward forex payments. Over a period of 10 months the five businesses made import payments of over MK3 billion. It was further noted that the accounts were active over a period of time when the outward forex payments were being made. Surprisingly, after enquiries into the nature of the businesses were made, this trend stopped and the accounts became dormant which showed a likelihood of the accounts being opened to illegally externalise foreign currency disguised as import payments.

Subsequent action

Investigations

Closure of the accounts

1.7.3 Typology 3: Use of new payments methods; Prepaid cards, Mobile money

Introduction

Over the years, there has been an increase in the use of New Payment Methods (NPM). These are the new and emerging non-traditional methods besides cash and cheque payments. They include point of sale (POS), prepaid cards, internet payment systems and mobile money payments.

While NPMs are becoming more widely used and accepted as alternative methods to store value and initiate payment transactions, it has been noted that the methods are misused and pose a money laundering and terrorist financing threat with the global COVID19 pandemic raging during the 2019/2020 period, there was a growing trend in the use of NPMs in Malawi. This section will highlight three typologies associated with misuse of the NPMs.

Additionally, during this period, the FIA analyzed successful fraud reports from one mobile operator between May and June 2020. The individual fraud case may not appear to be very significant, but the extent of the fraud is significant. For instance, an estimate of MK1 billion may have been stolen from mobile money subscribers and agents through their bank account electronic wallets and phone numbers.

1.7.3.1 NPM 1: Use of mobile money payment methods

Introduction

One of the mobile money operators in Malawi submits successful fraud[3] reports periodically to the FIA. For the period under review, the FIA observed fraudulent activities through the use of mobile numbers. According to the reports received, fraudsters further used voice, short message service (SMS), or both to communicate with the victim. The fraud is carried through the use of mobile subscribers, agents and SIM card swapping. The scams took advantage of the Corona virus pandemic which was one of the drivers of embracing use of mobile money. For example, fraudsters made calls and claimed to offer financial help while in the process of getting personal information to defraud the victim.

Regarding mobile money payments, both agents and individual subscribers use electronic wallets to enable them make transactions. The transactions may include; sending, remitting funds and making payments for products and services. Subscribers start transacting through their accounts once the account is connected to their mobile number.

[3] Successful frauds mean the attempts that were successfully executed by fraudsters

On the other hand, Subscriber Identification Module (SIM) card swapping fraud occurs when scammers take advantage of the weakness in the two-factor authentication and verification in which the second step is a text message (SMS) or call to a mobile phone number. In the incidents of fraud, SIM swapping can be used to take over someone's financial accounts.

Cases Summary

Offences	Cash and identity theft
Customer	Individual subscribers, agents
Instruments, methods and techniques	Cash remittances through electronic wallet, electronic transfers
Indicators	Transactions are conducted with speed. Initiator always expresses the urgency of the transaction. Requests about KYC details and change pin process. Calls about goods stuck at the borders. Requests for refund of money sent wrongly. Unusual text messages about bonuses and winning competition. Calls claiming someone's close relation had an accident and there is urgent need for money. Failure to make a call or send a text. Notification of an activity not known to subscriber. Failure to access the account.

1.7.3.1.1 Case study: Identity theft fraud

Case description

Mr. X posed as a staff member of YZ University. With this identity, he called Mr. Kaka (victim, not his real name). Apparently, Mr. Kaka has a son who is a student at YZ University. During the mobile phone conversation, Mr. X hinted to Mr. Kaka that his son had an outstanding fees balance of MK500,000.00 with the University. He further advised Mr. Kaka to send the money using the phone number that he used to call Mr. Kaka with.

Convinced with this phone call, Mr. Kaka sent the purported outstanding amount to Mr. X. However, Mr. Kaka failed to get hold of Mr. X after the money was successfully sent. Further inquiries established that the number was blocked. It was later confirmed that Mr. Kaka had been defrauded by an identity theft fraudster.

Subsequent action

Report sent to Mobile Money Operator

1.7.3.1.2 Case study: Know Your Customer (KYC) details update fraud

Case description

In a different mobile money fraud, Person A, a subscriber of MMO (Mobile Money Operator) B, one of the MMOs in the country received a call advising him to update his details with MMO B. The caller pretended to be an employee working for MMO B. The purported employee asked Person A to provide the details of his mobile money account with MMO B and bank account Person Identification number (PIN) in order to successfully complete the process of updating his account.

He was told and believed that the process was going to help him to transact on another mobile platform that is provided by Bank A. After Person A had provided the details, an amount of MK700,000 was transferred from his account wallet.

Subsequent action

Report sent to Mobile Money Operator

1.7.3.1.3 Case study: Use of refund method

Case description

In another case, Mr. Golo (not his real name) a subscriber with MMO B received a phone call from caller XYZ. The caller claimed to have wrongly sent MWK 100,000.00 to Mr. Golo's electronic wallet. He further specified that his aim was for Mr. Golo to return the money. Following this and without checking his account balance, Mr. Golo immediately transferred the specified amount to the wallet of XYZ. After sending the money, Mr. Golo tried to call XYZ to confirm receipt of funds but failed to reach the number as it was out of reach.

This failure made Mr. Golo to be suspicious which prompted him to check his account balance. To his amazement, there was no amount in his account that XYZ had earlier claimed to have mistakenly sent into his account. He then called MMO B who confirmed that XYZ might have been a fraudster.

Subsequent action

Report sent to Mobile Money Operator

1.7.4 Typology 4: Use of Prepaid Express Cards

Introduction

Another important trend noted under NPM is the use of prepaid express cards. Some commercial banks have opened up internet payment service for their customers to enable them to make payments, send and receive funds via smartphones and the internet. This has also seen a growing number of online purchases outside Malawi. A worrisome trend has been noted on the misuse of this platform where some individuals have accessed multiple accounts and multiple cards which they use to transfer funds.

One financial institution has a mobile application that allows its customers to transfer funds and make payments abroad from a bank account using a smartphone. The platform uses virtual express card on which the customer can load funds up to USD500 (about K368, 500) at a time.

This being a new platform, it is available to limited banks and a few customers, it has also been noted that some individuals who are not on this platform have been duped and defrauded. Fraudsters have been offering unsuspecting victims to use the platform. Once the victims deposit funds, the fraudsters have been evasive.

As the new payment methods continue to emerge and gain momentum, it is important that regulators and AML/CFT compliance professionals should understand the ML/TF risks associated with such products. Mechanisms to control the risks are of paramount importance in the AML/TF regime.

1.7.4.1 Case study: Structuring funds for cross border transfers

Case summary

Offences	Money laundering
Customer	Individuals
Instruments, methods and techniques	Bank accounts, master pass QR code, fictitious invoices
Indicators	Amounts being credited to the account not corresponding to amounts on invoices. Frequency of deposits not making sense. Timelines on invoices not tallying with timelines of credits. Invoices made out to an individual and payments coming in from multiple individuals. Source of funds on KYC declarations different from purported reason for payments.

Case description

The FIA investigated a case in which person X is a citizen of Country B but working in Malawi. Person X has a savings account with Bank G and his KYC documentation declares his source of income as his salary.

In a period of about one month, person X received various sums of US dollars from six different individuals in country B totaling to $46,059.57. The deposits were through the platform called Master Pass which is an e-payment platform that allows clients to use their own bank's mobile banking application to make payments from their bank accounts securely.

Investigations established that person X runs a general dealing business besides his employment. However, this business does not appear anywhere in his KYC documentation. Person X sent out invoices to J, one of the six individuals who made payments into X's account from country B. However, payments were made

to person B's account from six different individuals including J. The payments were purportedly regarding to the invoices.

Strangely, the payments were made very frequently (some up to 3 payments in a day by the same individual) and in small equal amounts, relative to the invoiced amounts. In addition, it was established that these individuals sending money to person B had their accounts marked not to send money outside of country B but were sending out invoices to a company in country B owned by one of the six individuals. The company's owner in return would credit person X's account through the Master Pass platform.

When Bank G called person X for an interview, he explained that the payments were for motor vehicle parts which he had sold to J as well as payment for land that he acquired for J. However, the money being paid into X's account and the invoices issued did not make sense. Further, the invoices submitted by X as proof did not match the invoices used for the payments. The timelines of the issuance of the invoice and the payments were suspiciously not tallying.

Subsequent action

Further investigations into the matter are ongoing

1.7.4.2 Case Study: Externalization of funds through Express Cards

Cases summary

Offences	Trade Based Money laundering (TBML)
Customer	Individuals
Instruments, methods and techniques	Cash, internet payment, smart phones, internet
Indicators	Large Cash Deposits. Third Parties with no distinct or defined relationship to customer. Credits followed by immediate and multiple debits.

Case description

In May 2020, Mr. CE applied and linked his bank account to internet payment platform. Following this linkage, activities in the account increased tremendously. The account started experiencing daily cash deposits from multiple sources which were followed by outward remittances through the express card. Multiple and

structured transactions could be done in a day based on the card limit. Later, due to a loophole in the system, the platform could allow Mr. CE to purchase multiple cards on the same account. This enabled Mr. CE to transfer funds outside Malawi in excess of MK90 million. The funds were sent to various destinations allegedly for importation of various goods including Personal Protective Equipment for COVID-19, electronics and second hand clothes. The account had no corresponding transactions to show payment for customs tax on the goods purported to have been imported into the country.

The case was reported to the regulator to look into the controls that safeguard the platform. Also, it was reported to law enforcement to investigate the purported importation. When Mr. CE was confronted he only managed to show proof of goods worth less than MK30 million to have been repatriated and received in Malawi. This suggests that payments for the rest of the goods was done in order to facilitate Trade-Based Money Laundering (TBML) and externalization of funds. Preliminary investigations also established that Mr. CE was used as a nominee to be sending funds outside Malawi by a foreign national. Third party beneficiaries were using the account by depositing the funds which were being loaded on the express cards.

Subsequent action

Further investigations into the matter are ongoing.

1.7.4.3 Case Study: Inward Transactions through Express Mobile Payments

In another case, Mr. MM a Malawian of foreign descent had his bank account linked to the internet. Through his account he was able to receive funds from outside Malawi. Through a suspicious transaction report, it was established that Mr. MM was regularly receiving funds from multiple sources from a neighboring country. There is evidence that the neighboring country has been experiencing devastating economic and foreign currency challenges. Therefore, inward flow of funds from such a country did not make economic sense. Within a month, over 51 transactions were made into the account, worth over K370 million (USD 501, 905) on some days over 5 transactions were made from one source.

Preliminary enquiries on the transactions alleged that the funds were proceeds from cement exports to the neighboring country. He, however, failed to produce documents to support this claim. Further trail of the funds established that Mr. MM was regularly applying for forex as foreign travel allowance at one of the financial institutions. The amount of the forex being applied were commensurate with the

amounts that Mr. MM was receiving from the neighboring country. The matter was disseminated to a law enforcement agency for further investigations.

Subsequent action

Further investigations into the matter are ongoing.

1.7.5 Typology 5: Financial Institutions Fraud

Introduction

In addition, the FIA observed a continuing trend in occupation fraud or employee fraud in financial institutions for the year 2019/2020. Fraud remains a big threat to financial institutions and their customers. This kind of fraud is committed against the financial institution by its own officers, who are the very people entrusted to protect the institution's assets and resources. They do this by abusing their fiduciary positions for personal gain.

Furthermore, financial institutions like banks are more vulnerable to employee fraud because the fraudsters within the institution have all the access to large amounts of personal identification and financial transactional data, as well as customer accounts. Since the fraudsters are fully aware of the established controls, they easily find loopholes to circumvent established procedures to commit fraud.

The most common *modus operandi* of this kind of fraud is that fraudsters illegally transfer money from suspense accounts, customers' accounts into their accounts or multiple nominees whom are mostly friends, relatives or fellow employees. Once they have access of the funds they later layer the funds through multiple transfers or cash withdraws.

1.7.5.1 Case Study: Theft by servant of Financial Institution

Case summary

Offences	Identity and cash theft, money laundering
Customer	Individuals
Instruments, methods and techniques	Bank accounts, remittances
Indicators	Government funds being transferred without supporting documents. Use of third parties in property transactions

	Transferring of funds to nominees.

Case description

During the period under review the FIA received an STR from one of the banks relating to fraud perpetrated by insiders. Mr. Bengo (not real name) was an employee of XYZ Bank as Manager at one of its branches. He defrauded the bank of an amount totaling MK45 million. By virtue of his position, Mr. Bengo was the overall in charge of bank services and operations at the branch and had access to the core banking system. Taking advantage of his powers, Mr. Bengo deceived his subordinates to transfer funds into the suspense account of which he was the sole authorizer of any transactions. He also stole his subordinate's credentials which he used to post transactions into the suspense account.

After successful transfers of funds into the suspense account, he then credited the funds into accounts of his nominees who were his friends. The friends would later withdraw the money and eventually give it to him. Not only did they give the money to Mr. Bengo, but they also purchased high valued items such as motor vehicles. It was noted that out of the total MK45 million that was stolen, MK40 million was stolen from the XYZ bank's vault. On some occasions, the funds were directly transferred to his account domiciled at ABC bank. The matter was reported and is still under investigation.

Subsequent Action

Ongoing Investigation.

1.7.5.2 Case Study: Theft through computer intrusion by an IT Manager

Case summary

Offences	Identity and cash theft, abuse of office, forgery and money laundering
Customer	Individuals, Financial institutions
Instruments, methods and techniques	Electronic Funds Transfer (EFT), cash theft, withdraws
Indicators	Transferring funds from suspense accounts. Stealing the funds from the bank vault.

	Transferring the funds to nominees. Forging loan application documents. Forging customers' information.

Case description

In August 2019, the FIA was in receipt of an STR which unveiled a syndicate of employees in Bank X who defrauded the bank of an approximate amount of MK47 million. Mrs. A, an IT expert was employed by Bank X as a Systems Administration Manager. By virtue of her position, she was fully aware of the administrative credentials necessary to gain access, modify settings and control all computer systems at the bank. Using this as an opportunity, Mrs. A created an economic unit which comprised of 5 individuals including some of her workmates to defraud the bank.

Through the employment of her IT expertise, Mrs. A breached the core banking system by making transfers to the accounts of the aforesaid four workmates in the form of loans. On face value, the transactions appeared normal as they had all the necessary entries for a loan application such as reviews and authorization. As a result, it was difficult for the frontline officers to detect the scam.

When the money got into accounts of her nominees, they periodically withdrew the money and gave it to Mrs. A. In other circumstances, they systematically made cash deposits into her account. The issue was detected when one of the nominees wanted to withdraw money at one of bank's local branches; however, the senior manager at the branch was suspicious of the transactions. This manager later promptly reported the matter to their Head of Risk and Compliance. The internal investigation uncovered the syndicate and the matter was eventually reported to Police.

Subsequent Action:
Arrest

1.8 EMERGING TRENDS

This section considers the emerging trends, and identifies the new typologies for money laundering that have been observed in the 2019/2020 financial year. It describes the typologies and illustrates the red flags or indicators of the predicate offences.

1.8.1 Typology 6: Money or Value Transfer Services

Introduction

The Financial Action Task Force (FATF) defines Money or Value Transfer Services (MVTS) provider as any natural or legal person who is licensed or registered to provide MVTS as a business, by a competent authority, including through agents or network of agents. The MVTS can further be categorized as part of Money Services Business in AML/CFT regime. MVTS refers to a financial service that accepts cash, cheques, other monetary instruments or other stores of value in one location and pays a corresponding amount in cash or other form to a beneficiary in another location. Examples of MVTS include; dealers in foreign exchange, cheque casher, issuer of traveler's cheque or money orders, money transmitter and also, provider and seller of prepaid access, payday lending and bill payments.

The MVTS are an option for money launderers and terrorists as they provide a quick and inexpensive way of remitting money and currency exchanges either within or outside a jurisdiction. However, the risk of MVTS to ML/TF depend on the extent and quality of the regulatory and supervisory AML/CFT framework as well as the implementation of risk-based controls and mitigating measures by each of the MVTS provider. Furthermore, the business nature of MVTS is that they do not maintain a long-term business relationship with their customers. As a result, detection of suspicious and unusual transactions become challenging.

Despite the fact that MVTS utilize the internet to make the transfers, it may be noted that a significant proportion of transactions involving the remittances are conducted in cash, especially at the sending and receipt point. Cash transactions are high risk in their nature. They are also more difficult to trace and at some point, transactions cannot be reversed. This limits the impact of controls that are designed to detect unusual and suspicious patterns after a transaction is done. In addition, MVTS do not immediately remit the relevant amount to the business at the receiving end; instead, they rely on the settlement of accounts over a period of time. This kind of operation creates a challenge in tracing financial flows from a specific sender to the ultimate beneficiary of a transaction.

During the year under review, FIA received STRs that showed a significant number of subjects who appeared to be using MVTS as a mode of transfer of ill-gotten money. The analysis of the STRs identified not more than 27 STRs, all involving cross-border transfers from or to countries such as Malawi, Zimbabwe, Uganda, Kenya

and South Africa. These are the countries where Company Q, one of the MVTS Operators in Malawi, has its presence and operations.

Out of the total 27 analysed cases, 9 were on Mass Marketing Fraud (MMF) - to be more specific, cyber-frauds. MMF happens when criminals explore online communication to develop trust and persuade individuals to give up their money. On the other hand, cyber-frauds or cyber-scams are types of fraud that exploit mass communication technologies. Examples of cyber-frauds include; foreign lotteries and sweepstakes, 419 scams and romance scams.

1.8.1.1 Case study: The use of MVTS to remit ill-gotten funds from Mass Marketing Fraud (MMF), especially cyber-scams.

Case summary

Offences	Mass Marketing Fraud (MMF), Cyber-fraud or cyber-schemes, Money laundering
Customer	Individuals, agents
Instruments, methods and techniques	Wire-transfer, Foreign currency notes, Cash withdrawals
Indicators	An increase in incoming funds activity for an individual with no history of such activity or where the stated business of the customer does not guarantee it. Dormant account suddenly receive incoming transfers followed by immediate withdraws. Non-face-to-face communication between agent and sender. Use of false name and fake social media account by agent.

Case description

From the analysis of the STRs received from MVTS, 9 out of 27 STRs, representing 33% depicted a pattern on cyber-fraud using a social media platform of

Facebook. These were done at different time periods. Fraudsters resident in Malawi created Facebook accounts and enticed Malawians who are in diaspora by making them believe that they were agents with Company Q. Company Q is a MVTS that is well known to provide affordable remittance services. A good number of Malawians working in countries where Company Q has agents use it for remittances.

After successfully getting in touch with unsuspecting victims, the purported agents went further to ask the victims to create transaction accounts indicating the beneficiary of the funds they were remitting the funds to Malawi. Following the creation of the transaction accounts, the fraudsters communicated to the victims that they had successfully created a transaction account for their beneficiary. However, unknown to the victims, the name of the beneficiary was changed from the one instructed by the victim to the name of the fraudulent agent. Some agents replaced the names with their own beneficiaries. The victims later learnt that their intended beneficiary did not get the funds and launched a complaint against Company Q. Further analysis established that;

- All the victims from the analyzed 9 STRS cases are based in one country besides Malawi. On the contrary, all the fraudulent agents and their beneficiaries are resident in Malawi.
- The first contact between the fraudulent agent and the victims was through social media platform, Facebook.
- All the analysed 9 fraud cases happened during the COVID-19 lockdown period that happened in the country where the victims are based. A possible explanation for this might be that the victims were desperate to send money to Malawi and hence fell on the traps of the fraudsters.

Subsequent action

Ongoing investigations.

1.9 PREVALENT TRENDS

1.9.1 Typology 7: Use of false documents

Introduction

Among the various money laundering methods and trends, use of false documentation keeps on re-emerging. Over the past 2 years, there has been increased utilization of falsified documents in financial transactions.

This section will focus on two areas of utilization false documents as follows:

- Falsified cheque and identification; and
- Opening and operating bank account with false documents.

For the 4 case studies that are detailed below, the red flags and indicators are summarized in the table below.

Cases Summary

Offences	Fraud
Customer	Individuals
Instruments, methods and techniques	Cash, Foreign cheque Cash
Indicators	Use of false identification documents. Customer making large cheque deposits despite having no known source of income. Customer 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 of a large amount of funds in cash. Large amounts of money withdrawn in cash from other accounts associated with this business.

1.9.1.1 Case Study: Use of falsified documents to open and operate a bank account

Case description

In November 2019, Mr. H opened a business account for Company Y009 with a branch of GH Bank. The account was authorised and opened by GH Bank. Just a

day after opening the account, Mr. H brought a foreign cheque of EUR989,000 to the bank for clearing. Since the cheque was of a foreign bank, the bank officer had to work with officers from cheque verification section to analyse the authenticity of the cheque presented by Mr. H. However, unknown to Mr. H, it is believed that GH Bank no longer clears foreign cheques.

After realising that the clearing processing was taking a long time, Mr. H started pushing the team to expedite the clearing of the cheque. The rushing of this process meant flouting the bank's cheque clearing procedures. This raised suspicion, thus the team decided to verify the authenticity of the customer's account opening documents that the customer had furnished to the bank during the account opening process.

The following was determined from the document verification exercise:

- The identification documents were false
- The business registration certificate could not be traced in the registrar of businesses' database system.
- There were no supporting documents for the payment of the cheque

Subsequent action

Ongoing investigations

1.9.1.2 Case Study: Use of falsified cheques

Case description

In July 2019, on a Saturday, Mr. CH went to Bank HJ to withdraw money from his account using a cheque. The bank officer initiated the process of cheque verification against Mr. CH's bank account. It was discovered that the account balance in his account was lower than the amount that was drawn on the cheque. After being informed of the account balance, he told the bank officer that he came to the bank the previous day which was a Friday for a special clearance with a cheque from Bank XYZ. He further indicated that he was unable to follow up with the bank on whether the transaction was successful or not since the bank had closed earlier on Friday afternoon and hence his coming on Saturday to withdraw the money.

The bank officer initiated a verification process to determine the progress of transferring funds from bank XYZ to Bank HJ so that he could proceed with transferring funds into Mr CH's account. The cheque was confirmed with bank XYZ

at 10:30am. Later, at 12noon of the same day, bank XYZ informed bank HJ that the cheque was not legitimate.

Subsequent action

Ongoing investigations.

1.9.1.3 Case Study 8.3: Use of false details to obtain funds illicitly

Case description

In another case of falsification of documents, an accounts assistant defrauded his employer. Mr. Zawo Zatonse (not real name) was an accounts assistant working for Company OO. His duties included depositing funds realised from sales into the Company OO's business account. In addition, he also did bank reconciliations for the company.

On 1st April, 2018 he went to Bank LL to deposit funds for Company OO. He presented three deposit slips to the bank teller as follows:

- First deposit slip with his bank details (Account name and Number)
- Two duplicate copies with details of company OO

The bank teller conducted the deposit transaction by entering into the bank's system the details on the first (original) deposit slip and there after proceeded stamping two duplicate copies without paying attention to the details on the copies.

Company OO only discovered of the fraudulent transaction in 2019 when it was conducting end of year accounts reconciliations. After analyzing the accounts and deposits it was discovered that the accounts assistant used to prepare multiple deposit slips. The original deposit slip was in his name and the other two duplicate copies were written in Company OO's name. This made it difficult for the bank teller to pinpoint the difference, hence ending up stamping all the three deposit slips.

Subsequent action

Ongoing investigations.

1.9.1.4 Case Study 4: Use of false bank account number and name

Case description

In June 2020, a Non-Governmental Organization (NGO) called X, published a vacancy advertisement through mass communication channels of WhatsApp and SMS asking young graduates to apply for the position of COVID-19 preventive measures awareness officer. The vacancy notice had a list of instructions on how an aspiring job seeker was supposed to follow in order for his/her application to be considered by the organization. The first prerequisite was for the applicant to deposit a sum of $6 into the organization's bank account. The second prerequisite required the applicant to scan the deposit slip and application form after which they had to send the NGO through an electronic-mail address that was provided in the advertisement.

On 6 June, 2020 a young man went to bank JKL to make a deposit of $6 into the account of NGO X. Attached to his deposit slip was a job application form, which indicated that the organization was recruiting young graduates to take up roles of COVID-19 preventive measures awareness officer. The form indicated bank details of non-governmental organization X at Bank JKL account number X000XCB12 and an alternative mobile money wallet number 0132773393.

Once the bank teller entered the account number into the bank's system in order to deposit the funds into the organization's account it was discovered that bank JKL had no account for the organisation. The teller tried to search using the account name, hoping that the account number had some error. After the search using the name of the organization the system presented an account of a non-governmental organization, which was not exactly the same as the one on the deposit slip. However, the account numbers bore some similarities. In summary, the account names were the same, but the numbers were slightly different.

Further investigation, revealed that desperate times due to the Corona virus pandemic provided a perfect opportunity for scammers to take advantage of job seekers desperation. The fraudsters used a legitimate name of the NGO but wrong bank account number. Their intention was to ensure that when a victim failed to deposit money to the wrong account, they would alternatively use the mobile money platform to send the money. The number for the mobile money was already provided as an alternative in the advertisement.

Scammers conducted fraudulent activities by:

- Creation of an organization with an already existing NGO name.
- Demand for application fee to be the main interest to swindle people.
- Provision of false bank details and alternative mobile account number.
- Obtaining a mobile money wallet number in the name of a different organization and not in the full name of the purported NGO.

2 RECOMMENDATIONS

The purpose of this section is to outline the recommendation to various stakeholders on the implementation of AML/CFT measures. These measures help in preventing, detecting and deterring money laundering and terrorist financing. The recommendations aim to address the gaps identified in the typology case studies noted in the period. Effective and efficient implementation of such measures will help in the fight against financial crimes.

1. **Improved verification of Know Your Customer documents in banks.**

Apart from the requirement of knowing the customer by financial institutions, reporting entities are also supposed to verify the information they collect for this purpose. Banks should ensure that they verify KYC details within a reasonable time after opening accounts. This will assist in identifying any anomalies that may be there regarding the real identity of customers before entering into a business relationship with them. It may also help to identify false documents that are deliberately furnished by would be financial crime perpetrators.

On the other hand, failure to verify such information may render transaction monitoring of the customers' activities difficult. Transaction monitoring is also a very important compliance procedure that assists in identifying unusual transactions. Therefore, such failure may result into the financial system being used by those perpetrating financial crimes.

2. **Improved detection controls**

Financial institutions should be on the lookout for fraud affecting both the institution and customers. This should assist in implementing necessary measures to be able to not only prevent but also to identify any complicity. For example, where financial institution employees collude with third parties, the financial institution should ensure continued Know Your Employee exercise for senior

management and junior employees. This would help in reduction of fraud, detection of financial crimes, and improvement of the reputation of the financial institution which would eventually have a positive effect on customer retention and business growth.

3. **Improved control environment**

Controlling officers in Government Ministries, Departments and Agencies should ensure that the availability of up-to-date controls to prevent, detect and deter the override of controls by employees. Apart from proper implementation, there should be ongoing training and awareness provided to employees regarding the controls and ways of improving integrity. There should also be a provision of whistleblowing opportunities for both internal and external informants.

Regarding ghost workers, the employer should ensure that proper controls are put in place to avoid remunerating undeserving individuals. On the other hand, financial institutions should monitor transactions to ensure they match with the information they have on the customer. In addition, bank account name should match with bank account number when crediting salary amounts.

4. **Improved AML/CFT controls in real estate sector**

The real estate sector is being utilised to invest proceeds of crime thereby laundering the funds. This is done through buying, selling and construction of property. As a result, proper measures should be implemented by regulators to ensure that proceeds of crime are not integrated into the financial system through real estate sector. Real estate sector should embrace regulation for both buying and selling of property as well as construction of real estate. Tax authorities are useful in establishing if funds used for buying or construction of major real estate were subject to taxation in previous three to four years. In addition, legal practitioners should ensure that appropriate customer due diligence is conducted when conducting conveyancing transactions.

5. **Foreign exchange control**

Regarding foreign exchange control, financial institutions should continue to ensure requesting and scrutinising all the supporting documents accompanying a foreign currency remittance application. Apart from this, financial institutions should also identify and scrutinise applications for transactions that appear not to make business sense. Further, proper due diligence measures should be performed above and beyond the normal course of business transactions for transaction that are suspicious.

6. **ML/TF awareness**

There should be continued awareness by service providers to their subscribers of notable fraud possibilities. Emphasis should be noted on the amount of funds that individuals may lose due to fraud. The same should be done by financial institutions regarding the introduction of new products and services. Under this awareness effort, the general public is alerted to the following:

- Not to allow others to use them in conducting transactions they do not understand
- To provide the required information to FIs when requested
- To report to FIA or LEAs if they suspect wrongdoing
- To verify with their relevant FIs before making payments etc.

3 CONCLUSION

In conclusion, it was noted that there are continuous trends such as theft of public funds and financial institutions fraud to mention but a few. Despite continued efforts that the FIA and other relevant stakeholders implement to curb these vices, it has been observed that there is need for concerted efforts and collaboration from all parties involved in order to reduce financial crimes. With such efforts, prevention, detection and deterrence will be achieved. Also, collaboration and exchange of relevant information, knowledge and skills among law enforcement agencies will result into the desired outcomes.

With prevalent trends, the FIA emphasises the need of continuous implementation of controls that identify false documents. One way is through verification of such documents. Important to note is that avoidance of implementing such controls may result in very costly consequences for both the businesses and individuals.