FINANCIAL INTELLIGENCE AUTHORITY

Making Malawi free of financial crimes

MONEY LAUNDERING TRENDS AND TYPOLOGIES REPORT

April 2022 - March 2024

Table of Contents

FIA GENERAL INFORMATION

Registered name	:	Financial Intelligence Authority
Postal address	:	Private Bag B441, Capital City, Lilongwe 3, Malawi
Telephone number	:	+265 111 759 141
Website	:	https://www.fia.gov.mw/
Email	:	info@fia.gov.mw

ACRONYMS AND ABBREVIATIONS

Abbreviations

ATM	Auto-teller Machine
AML/CFT/CPF	Anti-Money Laundering/ Combating the Financing of Terrorism/Combating Proliferation Financing
FATF	Financial Action Task Force
FCA	Financial Crimes Act
FIA	Financial Intelligence Authority
KYC	Know Your Customer
LEA	Law Enforcement Agency
ML	Money Laundering
MVTS	Money and Value Transfer Services
NPM	New Payment Methods
PF	Proliferation Financing
POS	Point of Sale
SBML	Service-Based Money Laundering
STR	Suspicious Transaction Report
TF	Terrorist Financing
TBML	Trade-Based Money Laundering
VAT	Value Added Tax

1 INTRODUCTION

The Financial Intelligence Authority (FIA) continues to make strides in its effort of fighting financial crimes as per its mandate given under the Financial Crimes Act (FCA), 2017. The FIA has been in existence for 17 years and plays a very important role in fighting financial crimes. One of the efforts is the production of the Trends and Typologies Report. The report is issued pursuant to Section 4(d) of the FCA. The law provides for the FIA to conduct research into trends, techniques and developments in financial crimes including Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF). The FIA has been producing trends and typologies reports since 2011. Apart from being obligated by the law in Malawi, best international AML/CFT/CPF practices also require Financial Intelligence Units (FIUs), to conduct strategic analysis. Notably, the trends and typologies report is one of the products of that analysis.

The trends and typologies report helps in providing insight and better understanding of activities, behaviours, type or category of individuals involved, geographical locations, methods and reasons for activities in relation to ML, its predicate offences, TF and PF. The analysis gives oversight that helps in informing significant AML/CFT/CPF policy makers in making effective decisions. The analysis is also forward looking as it can be predictive. As a result, responses to events are developed and planned even before such events happen. In addition, relevant stakeholders can effectively allocate human and financial resources as a response to the ML, TF or PF trends. Proper allocation of resources targets identified strategic problems and results in effective use of such resources. The report may also be used for different awareness programs that are carried out by different stakeholders in AML/CFT/CPF.

The FIA produces the report periodically. The current report covers a period between 2022 and 2024. The FIA observed some continuing ML and TF trends from the prior period and new emerging ML and TF trends in the current period.

Continuing trends were observed in the following areas: theft of public funds, foreign currency exchange control violations, financial institution fraud perpetuated by employees, corruption, fraud, tax evasion and abuse of New Payment Methods (NPM). Emerging trends were noted in the following areas: use of lawyers to facilitate ML, use of third parties to facilitate ML and TF, and resurfacing of standalone ML.

Unlike the previous reports, the current typologies report includes a section on asset recovery efforts employed in the period. The section focuses on highlighted cases and notable achievements and challenges encountered in asset recovery efforts. The cases detail the recovered proceeds of crime, instrumentalities of crime or property of corresponding value (equivalent benefit).

Overall, the FIA believes that the information contained in this report will go a long way in reaching its intended purpose of fighting ML, TF, PF and other financial crimes in Malawi.

2 EXECUTIVE SUMMARY

The 2022-2024 Trends and Typologies report presents different methods used for ML and TF over this period. These methods are important as they inform decision making in AML/ CFT/ CPF related undertakings. They also assist in the formulation of specific solutions to peculiar challenges faced by different stakeholders. For instance, the identified methods assist in informing the updating of the National ML/TF/PF Risk Assessment. Specifically, the report assists in proper assessment and understanding of the threats identified from the isolated methods in the report. The methods were categorised according to how often they were identified by a reporting entity.

The report identified continuing trends as those cross-cutting over a period before 2022. To be more precise, these trends are always there as they are common predicate offences for ML in the country. Those identified during the period under consideration were; exchange control violations through abuse of VISA debit cards, general theft and theft of public funds, fraud, use of new payment methods, financial institution fraud perpetrated by employees, corruption and tax evasion.

The report further identified emerging trends in the period. These are a collection of methods that were not identified before but manifested in this period. These were use of third-party accounts to conceal illegally gotten funds, use of lawyers to launder proceeds of crime, standalone money laundering, terrorist financing and Service-Based Money Laundering (SBML). On the supervisory part, the FIA noted some de- risking trends that happened during the period.

The FIA continues to note that the disparity between the authorised and parallel market rate for foreign currency exchange has brought different abuse methods for exchange controls. The number of STRs that the FIA

received in the period relating to exchange control violation surpassed the number of STRs for other predicate offences. In addition, this has been a continuing trend from the previous periods.

3 OVERVIEW OF STRs RECEIVED

3.1 General observations from STRs and Financial Investigations

Suspicious Transaction Reports (STRs) are an important source of information for this report. This is because their analysis uncovers predicate offences related to money laundering and other financial crimes. In addition, the analysis may reveal illicit sources of funds and criminal proceeds. Intelligence derived from analytical work and financial investigations is then shared with the appropriate Law Enforcement Agencies (LEAs).

Through this process; patterns, methods and trends of criminal activity are uncovered along with vulnerabilities and indicators of ML/TF, techniques.

For this report, the FIA used information from these sources;

I. STRs that were received and analysed from various reporting entities under AML/CFT for the period between April 2022 and March 2024. The STRs were filed with the FIA by financial institutions, Designated Non-Financial Businesses and Professions (DNFBPs and the general public. The total number of STRs analysed for this report was **357.** These are summarised in the table below:

Table 1: Summary of STR subject

No	STR subject	Count
1	Abuse of exchange control	180
2	Fraud	37
3	Tax evasion	90

4	Corruption	3
5	Theft (including theft by public servant)	34
6	Abuse of lawyers	5
8	Standalone ML	4
9	De-risking by reporting entities.	4
	Total	**357**

II. Requests for information from LEAs
III. Media reports and other open sources
IV. Publicly available information
V. Previous trends and typologies reports
VI. Sanitised cases from LEAs.
VII. Information provided by other FIUs.

3.2 Common Indicators Observed

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

- Large deposits into bank accounts beyond the declared income, profile and transaction history.
- Immediate withdrawal of funds in other jurisdictions through ATMs and merchant point-of-sale machines soon after deposit.
- The person exercising control and ownership of a bank account different from the one who opened it.
- Use of false invoices to claim Value Added Tax (VAT) refunds from Malawi Revenue Authority (MRA).

- Use of third parties to conceal beneficial owners of the funds.
- Use of forged car ownership documents as security to obtain bank loans.
- Use of invalid invoices to obtain foreign currency and externalise it.
- Sending foreign exchange outside the country for payment of goods that were not imported into the country.
- Use of false information to open bank accounts
- Procurement fraud through reluctance of management to follow up on the selection processes of the supplier such as lack of minutes for Internal Procurement and Disposal Committee (IPDC) meeting for procurement processes and unauthorised signatories on contracts.
- Business Email Compromise (BEC) through scammer's disguise of official email addresses.
- Subjects attempt to distance themselves from a transaction by creating various levels of transactions.
- Use of personal bank accounts instead of business accounts.
- Operating unregistered businesses.
- Use of vulnerable individuals to easily manipulate them in externalising or laundering funds.
- Multiple third-party cash deposits into the same account followed by outward international transfers to multiple individuals.
- Narrations on the transfers made not reflecting the declared purpose of transactions.
- Employees fraudulently processing cheques by flouting procedures.
- Customers depositing funds into their accounts, but the deposits not reflecting in their bank statements.
- Bank employees falsifying or forging procurement documents such as quotations to create a misleading appearance that the bank had legitimately procured goods from suppliers.
- Huge cheque and cash deposits immediately followed by transfers

- Huge transactions involving Politically Exposed Persons (PEPs)
- Willingness to pay the extra charge for speedy access to funds.
- Under-declaration of imported goods
- Multiple invoicing for the same shipment
- Using fake or fictitious invoices
- Use of a deceased person's identification document
- Unusual request for quick execution of court order.
- All transfers from mobile money account resulting in cash withdrawals by the recipients.
- Existence of transactions not related to the declared business
- Roundtripping (i.e. sending money to a third-party account and then having it returned in the form of a non-taxable transaction, such as a gift or loan).

4 MONEY LAUNDERING, TERRORIST FINANCING TRENDS AND TYPOLOGIES

4.1 CONTINUING TRENDS

4.1.1 Typology 1: Exchange Control Violations through abuse of VISA debit cards

Trading and use of foreign currency in Malawi was governed by the Exchange Control Act of 1989 and its subsidiary legislation, the Exchange Control Regulations. Currently, the exchange control violations are governed by the Exchange Control Act of 2025 and foreign exchange directive, 2025. Government gazette notice number 86 of 2025. The Regulations provide for travel and business allowances. The regulations stipulate that Authorised Dealer Banks (ADBs) may approve applications for business, holiday or medical travel allowances up to USD10,000 or the equivalent thereof in any other currency. Travel allowances of up to USD 3,000 may be granted without requiring production of documentary evidence of travel other than the applicant's

passport. Applications for any travel allowances in excess of USD 3,000 must be supported by a bus/air ticket or vehicle police clearance report in the case of those travelling on private vehicles as evidence of travel.

For VISA debit cards, the pre-approved limits, has provided an opportunity for illegal externalisation of funds, despite being a positive development. The FIA has observed common trends where bank customers are regularly depositing large amounts of Malawi Kwacha (MWK) through cash or Electronic Funds Transfers (EFTs). There would be a subsequent withdrawal of the funds in foreign currency through Merchant Point of Sale (POS) and Auto Teller Machines (ATMs) in foreign jurisdictions. In the period under review, the FIA analysed more than 100 STRs in relation to illegal foreign currency externalisation using the VISA debits cards. Further investigation and analysis established the following:

- About 80% of the accountholders involved are not cross-border traders.
- The accountholders do not have a Tax Identification Number (TIN) to be used for importation of goods.
- Use of fake air ticket to have their applications approved.
- Multiple accounts being credited by the same source.
- Opening of more business accounts away from the physical location of the declared business.
- Funds being deposited in locations away from where the business is located.
- Failing to explain the amount of goods purchased and the amount of money possessed before a cross-border trip.
- Funds being withdrawn through ATM and POS at same locations and same amounts.
- Recruitment of individuals to collect cards from friends, relatives and other unsuspecting villagers.

- One account having more than one active card without proper justification.
- Recruitment of bank employees to assist them in processing of cards and moving of funds from one account to another.
- Opening several business accounts for shell companies.
- Funds transfers into bank accounts usually higher than what was declared.

Case Study 4.1.1.1: Foreign Exchange Control violations through Abuse of Visa Cards

Case Summary

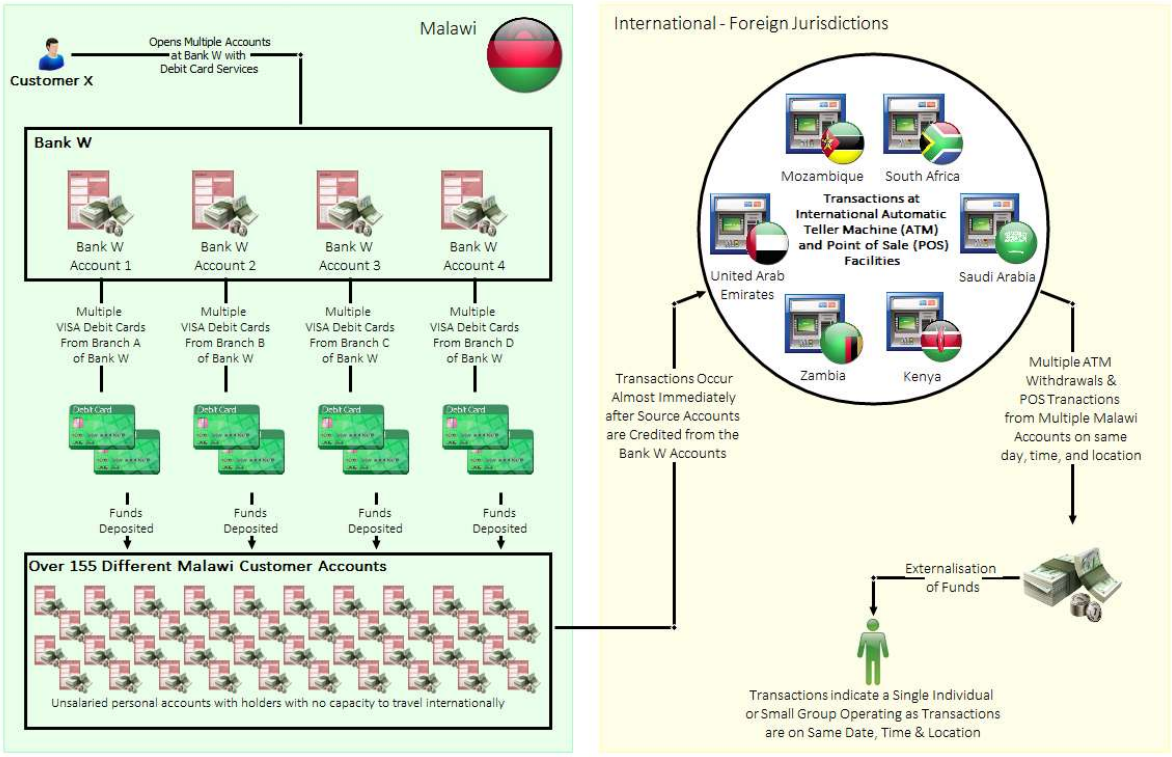
Offences	Exchange control Violation
Customer	Individual
Products & services	Bank accounts, ATM cards, cash
Channels	EFTs, remittances
Indicator	• Large deposits into account beyond the declared income. • Immediate withdraw of funds in other jurisdictions through ATMS and merchant POS. • The person exercising control and ownership of a bank account different from the one who opened it.

Case Description

Customer **X** of Bank **W** opened several accounts on behalf of third parties located in remote areas of the country. Customer **X** would then visit different branches of Bank W to obtain Visa Debit cards for the accounts that were opened. Upon opening the accounts and obtaining the VISA debits cards, customer **X** credited over 155 other customer accounts with money. The credits were followed by immediate cash withdrawal (within the same day the credits were made) on POS and ATMs in Zambia, Mozambique, South Africa, Kenya, and United Arab Emirates. The cash withdrawals on the accounts were made around the same time, date and ATM locations. The analysis of the account opening documents revealed that most of these accounts were unsalaried personal accounts, and their transactions did not match the declared income. Furthermore, the account holders appeared not to have the capacity to travel to some of the jurisdictions where the transactions were being made. This pattern makes it most likely that the accounts were being controlled by one individual.

Subsequent Action

Investigations and Arrest



Typology Visualisation- 1.6.1 Case Study
Withdraw of funds from border countries and further abroad

Case Study 4.1.1.2: Enticing unsuspecting third parties(villagers) to open banks accounts to be used for illegal externalisation of funds

Case summary

Offences	Illegal externalisation
Customer	Individuals
Products & services	Bank accounts, ATMS
Channels	remittances

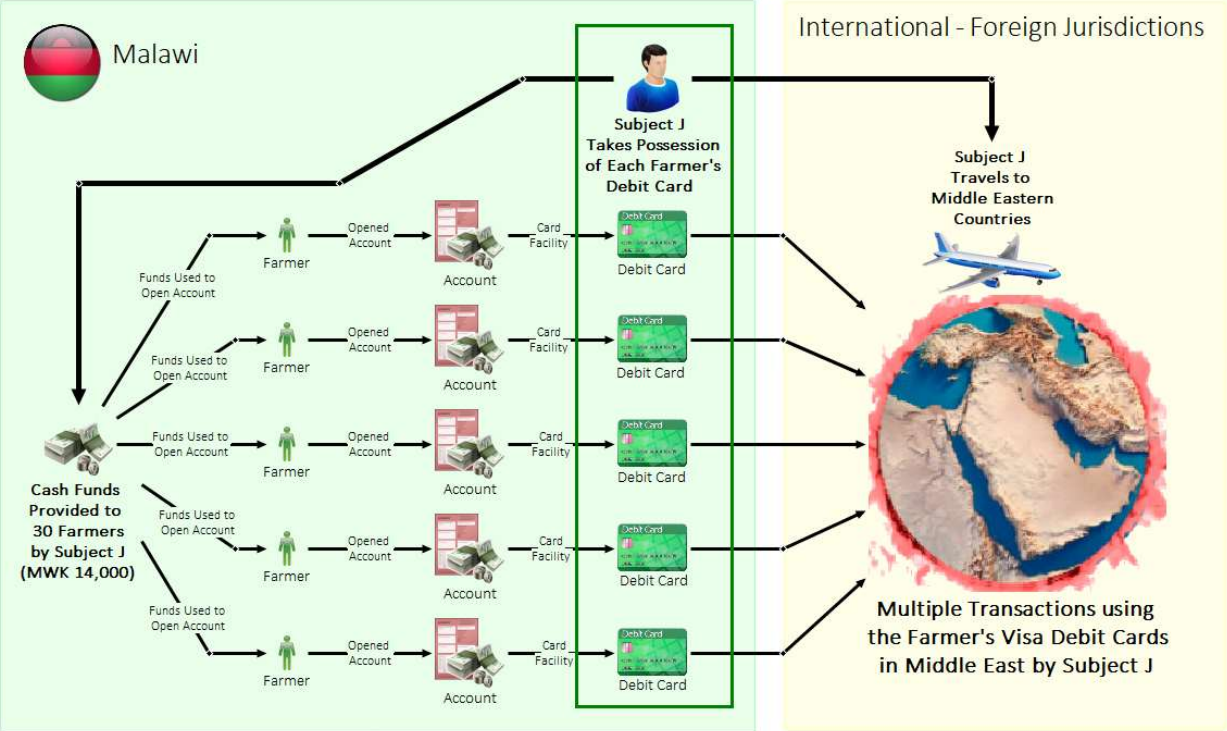
Indicator	• People from the same village open accounts on the same date and location. • All accounts being credited by one source. • Being found in possession of cards belonging to others.

Case description: Using third parties to open bank accounts

In 2023, Person J went to Village K and convinced over 30 unsuspecting small-scale farmers that she/he wanted to open bank accounts for them at one of the branches of bank F. Together, they went to the bank to fill out account opening forms. In addition, Person J gave each of the farmers an estimate of MWK 14,000 to cater for account opening processes and VISA debit card expenses. When the accounts were opened and the VISA cards issued, Person J collected the VISA cards from the account holders and told them that he/she would return them later. On the contrary, Person J travelled to one of the countries in the Middle East and transacted using the cards without the knowledge of the account holders after he had made deposits to each of the accounts.

Subsequent Action

Arrest and confiscation of cards.



Typology Visualisation-1.6.1.1B Case Study

Enticing unsuspecting villagers and other casual labours to open bank accounts to be used for illegal externalisation of funds.

Case study 4.1.1.3: Possessing several VISA debit cards without valid explanations

Case Summary

Offences	Exchange control violation
Customer	Individual
Products & services	Bank accounts, ATM cards, cash
Channels	EFTs, remittances
Indicator	• Being found in possession of multiple Visa Debit cards belonging to different people.

Case description: People arrested for being found with over 400 ATM cards of other people
In 2023, the FIA, Reserve Bank of Malawi (RBM), and Fiscal and Fraud Unit (FFU) of Malawi Police Service (MPS) investigated a case where some people were arrested by the police in 2023 for being found in possession of more than 400 ATM cards issued by various banks belonging to different people. The investigation revealed that the arrested people had recruited other people who collected Visa debit cards from various people across the country. After collecting the cards, they travelled to one of the Middle East countries where they made POS and ATM withdrawals. Furthermore, investigations revealed that while in the Middle East, the accounts were credited from the same source, with the same amounts (equivalent to the withdrawal limit) and from the same location. It was also discovered that the actual cardholders were paid between MWK10,000.00 and MWK20,000.00 for releasing the cards to be used by the perpetrators.
Subsequent Action Arrest, prosecution, confiscation of the debit cards and administrative sanctions.

Case Study 4.1.1.4: Registering Businesses and later opening business bank accounts to obtain premium visa cards to be used for forex externalisation

Case summary

Offences	Illegal externalisation of forex
Customer	Individuals, Businesses
Products & services	Bank accounts, ATMs
Channels	Remittances
Indicators	• Registering multiple businesses.

	• Opening business accounts and declaring high turnover to obtain premium Visa debits cards. • Large cash deposits from different sources followed by outward remittances. • Large deposits by different people. • Large deposits in different locations.

Case description

The FIA, RBM, and FFU investigated a case where Mr. X and his wife registered more than 80 shell companies within a space of two months. Upon registering the companies, they went to various banks where they opened more than 120 business accounts and eventually obtained multiple premium VISA debit cards which have high withdrawal limits. The accounts were opened in various branches. The accounts were mostly funded by large cash deposits from unknown sources and then later transferred into other numerous bank accounts in small sums. After these transfers, the funds were withdrawn in foreign jurisdictions on ATMs or through POS purchases.

Subsequent Action

Arrest

Closure of accounts

Case Study 4.1.1.5: Externalising funds using bank accounts and ATM cards of students studying abroad

Case Summary

Offences	Exchange control violation
Customer	Individuals
Products & services	Bank accounts, ATM cards, cash
Channels	EFTs, remittances
Indicators	• Large deposits into bank accounts of students studying abroad followed by withdraw of same amount in the country of study through ATM and POS purchase. • Deposits done by people not expected to be responsible for provision of stipend or expenses for the student.

Case Description

A Malawian student in Asian Country B, opened an account with Bank C based in Malawi. Over the years, the volume of transactions in the account changed significantly. The student was transacting more than what he had declared when opening the bank account. For example, for a one-year period, the student transacted over MWK 100 million. The account got huge cash deposits and electronic transfers from various individuals in Malawi. The credits were followed by instant ATMs withdrawals and POS purchases in the jurisdiction the student is based.

Subsequent Action

Investigations

4.1.2 Typology 2: Theft of Public Funds

Introduction

In the period under review, the FIA noted several trends relating to theft of public funds. These ranged from procurement fraud, financial statements misrepresentation, public officials transferred huge amounts of funds from government accounts to personal accounts. Oftentimes, these were using third parties as conduits to conceal the connection between the government account making the debits, the public official facilitating the transfer and the third parties' accounts being used.

During the period, there was a trend of unexplained frequent allowances being deposited in the accounts of public officials without proper supporting documentation. By employing the expenditure method of proof of legal income, it was discovered that these public officials had obtained unexplained wealth whose only logical explanation was theft of public funds.

Powerful public officials were seen to have fraudulently influenced award of procurement contracts to overseas companies. Analysis revealed that the companies that were awarded contracts were shell companies.

Case Study 4.1.2.1: Public Officers Fraudulently Influencing Granting of Procurement Contracts to an Overseas fictitious Company.

Case Summary

Offence	Abuse of Office
Customer	Individual/business
Products and services	Bank Accounts

Indicators	• Frequent reminders of payment from the Chief Executive Officer. • Absence of minutes of meeting from the Internal Procurement and Disposal Committee. • Unusual signatories on contracts. • Reluctance of management to follow up on the selection processes of the supplier. • Supplier's use of a non-business email address.

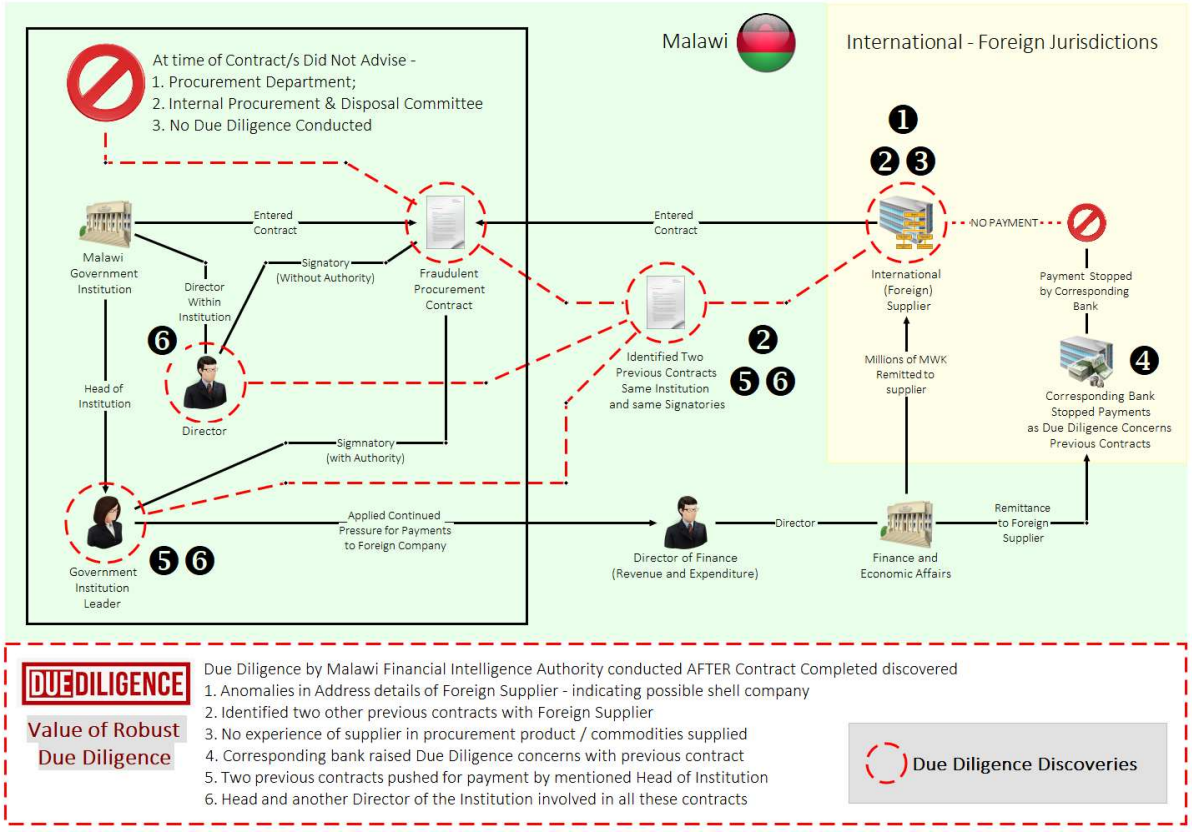
Case Description

A Government Institution found itself paying huge sums of funds to a foreign supplier after a fraudulent procurement contract was signed. The contract was entered into without the knowledge of the procurement department, or the Internal Procurement and Disposal Committee. The FIA intelligence discovered communication from the Head of the Institution to the Head of Finance pushing the latter to quickly make payment to the supplier. The Head of the Institution was following every step of the payment process until it was finally remitted to the supplier. In its investigations, the FIA conducted background checks on the supplier and noted that the address that was put on the contract was for a different company. In addition, the name that was used by the supplier was for a different company whose services were no way close to the services that were being offered in the contract. It was, therefore, concluded that the company that received these public funds was a fictitious company with no physical existence. Investigation uncovered two other contracts prior to this one, both being pushed for payment by the Head of the Institution through communications such as emails. One of the two contracts was paid but the corresponding bank in the

receiving country returned the funds after its due diligence raised suspicion of the entity being paid. The other contract was not paid at all as the Head of Finance refused to make payment without relevant supporting documents. In all these fraudulent contracts, the Head of the Institution, and one Director were signatories for the institution. However, the other director was not an approved signatory for contracts by the institution. Together with the Head of Institution, they took lead in the email communications and pushing for payment.

Subsequent action

Disseminated to Law Enforcement Agency (LEA) for investigations.



Typology Visualisation-1.6.2.1 Case Study

Powerful public officers influencing granting of fraudulent procurement contracts to oversee shell companies.

Case study 4.1.2.2: Public officials using third parties to siphon money from Government accounts

Case Summary

Offence	Money laundering
Customer	Individual
Products and services	Bank accounts and electronic funds transfers
Indicators	• Frequent significant credits from government account. • Client profiles not matching with the source of the funds. • Several accounts in different names using same phone number on KYC. • The transaction was inconsistent with the customer's profile.
Case description Person X siphoned money amounting to MWK 100 million from Government by using several individuals to open accounts using X's phone number as the contact number for all the accounts. These accounts were used to receive electronic funds transfers from the Ministry of finance. None of the account holders worked in civil service, nor had any business that would enable them receive money from the Ministry of Finance.	
Subsequent action Investigations to understand purpose of funds from the Ministry of Finance.	

Case study 4.1.2.3: Public official's misuse of public funds

Case Summary

Offence	Theft of public funds
Customer	Individual
Product and services	Bank accounts and electronic funds transfers
Indicators	• Transactions inconsistent with the customer's profile. • high volumes of transactions within a short period of time.

Case description

The FIA analysed a case involving a public official who opened an account with one of the banks. The account was used to receive salary from the Ministry of Finance.

The account started receiving frequent, huge transfers from Ministry of Finance. Further analysis revealed that within a short period of time, the account received MWK120 million. The funds were immediately withdrawn in cash, leaving no trail as to the eventual use after withdrawal.

Subsequent action

Freezing of bank account, preservation of funds and an arrest.

Case Study 4.1.2.4: Equity Contribution, Loans and Other Facilities

Case Summary

Offence	Fraud

Customer	Individuals, Businesses
Product and services	Bank accounts, Cheques
Indicators	• Significant loan write-offs. • Increased vested interests by high profile government officials in entity's dealing and operations.

Case description

Following a forensic report of a state-owned company, the FIA was part of a task force to investigate allegations of financial crime within the company. The allegations were on fraud, financial mismanagement and corruption in addition to an issue related to unaccounted for equity contributions. The Malawi government went into an agreement with a private investor to run a state-owned company as a joint venture. After some years, it was alleged that the private investor did not meet their part of agreement by failing to pay its equity share. Instead, the private investor used the company to obtain unauthorized government-backed loans.

It was alleged that the loan amounts were taken without Parliamentary approval. The loan was estimated at USD 118 million. In addition, almost USD 35 million of investment by the private investor as their part of the contribution to the joint venture was not accounted for. It was further alleged that there was flow of money from Malawi to foreign companies which later was injected back into the joint venture as capital contribution, when in fact the funds originated from a source within Malawi.

Subsequent action

Investigation and prosecution

Case study 4.1.2.5: Abuse of Government agency funds.

Case Summary

Offence	Theft of public funds
Customer	Individuals, Businesses
Product and services	Bank accounts, Cheques, Cash withdrawals
Indicators	• Frequent huge cash withdrawals. • Withdrawal methods not consistent with standard procedures. • Cash encashments to staff members. • Account used for paying suppliers ends up paying some employees.

Case description

The FIA analysed a case involving a government agency that opened an account with one of the banks in the country. The aim of the account was to pay suppliers through cheques and bank transfers and pay its employees' salaries through bank transfers alone. Within a period of 8 months prior to FIA's analysis, MWK 2 billion was paid to staff members in cash. Further to that, over MWK 5 billion was paid in cheque to other individuals, some of whom are staff members. The purpose of these transfers was not established.

The FIA also analysed a case involving another government agency, whose account was opened with a sole purpose of paying suppliers in cheque and bank transfers. The account had a sudden surge in immediate cheque encashments after every credit into the account. These withdrawals were made by common names who happen to be employees of the agency. On one occasion, a sum of MWK 72, 665, 000.00 was withdrawn in cash over the counter by the agency's employee.

Subsequent action

Case referred to National Audit Office (NAO).

Case study 4.1.2.6: Abuse of public funds through fraudulent allowances.

Case summary

Offence	Theft by public servant.
Customer	Individual
Product and services	Bank accounts
Indicators	• Frequent credits into bank accounts. • Several transactions on a day bearing same amount, and same description of "Allowance"

Case description

In 2022, the FIA analysed a case involving a Public Official X who was the Head of the Government Agency Z. Public Official X used his account to receive fraudulent allowances from Government Agency Z and its associated departments. X's name was found on every allowance sheet of the agency. These were the allowances into the bank account. Over a period of two years Public Official X had received over MK90 million in allowances. This was unusual because at X's grade, X was supposed to receive a maximum of MK18 million in a year assuming X was on allowance each and every day of the year. In Government subsistence allowance is only received when someone is working out of duty station. In X's case it would mean X was out of duty station every day. For instance, one day, X's account received MWK 2 million as allowance.

Subsequent action

Arrest of X

Prosecution

4.1.3 Typology 3: Fraud

Fraud is one of the common predicate offences happening in the country. Commission of fraud involves falsification of documents, misrepresentation of facts, abuse of position, failure to disclose information and details to have a financial gain or cause a financial loss. Recently, fraud offences have also been enabled by technology. For example, mobile money fraud and Business Email Compromise (BEC).

Case Study 4.1.3.1: Falsification of Documents

Falsification of documents involves intentionally modifying or altering of documents with a goal to deceive or circumvent specific procedures, processes or controls. The FIA noted an ongoing trend on the use of false documents in carrying out financial transactions. During the period, falsification of documents was commonly used in:

- VAT claim returns for refunds.
- Collateral documents to obtain a bank loan; and
- Invoices to externalise foreign currency.

Cases Summary

Offences	Fraud, Money Laundering.
Customers	Businesses and individuals
Products & services	Cash, cheques, funds transfers
Channel	Remittances
Indicators	• Use of false invoices to claim VAT refunds. • Use of third parties to conceal beneficial owners of the funds. • Large amounts of money being transferred to accounts belonging to individuals.

	• Customers transacting beyond their profile and transaction history. • Use of altered car ownership documents as security to obtain bank loans. • Use of invalid invoices to obtain foreign currency in order to externalise it. • Externalising foreign currency to purchase goods that were not imported. • Use of false information to open bank accounts.

Case Study 4.1.3.2: Falsification of VAT claim returns for refunds

Case description

A Non-Governmental Organisation (NGO) X, falsified Value Added Tax (VAT) claim returns for refunds. The Taxation Act exempts VAT on services offered by NGOs. The NGOs are allowed to pay VAT on the services and later claim that expense from the Malawi Revenue Authority (MRA). In other instances, the VAT is not paid to service providers upon the NGOs producing a VAT exemption certificate.

In this case, NGO X claimed that it was paying VAT for the services obtained from various entities. Later, it filled a VAT refund claim form with MRA. The VAT refund claim was supported with invoices and payment receipts from the service providers. The VAT refund claim was processed and a sum of MWK 200million was paid to NGO X. The funds were withdrawn using cheques from NGO X's account

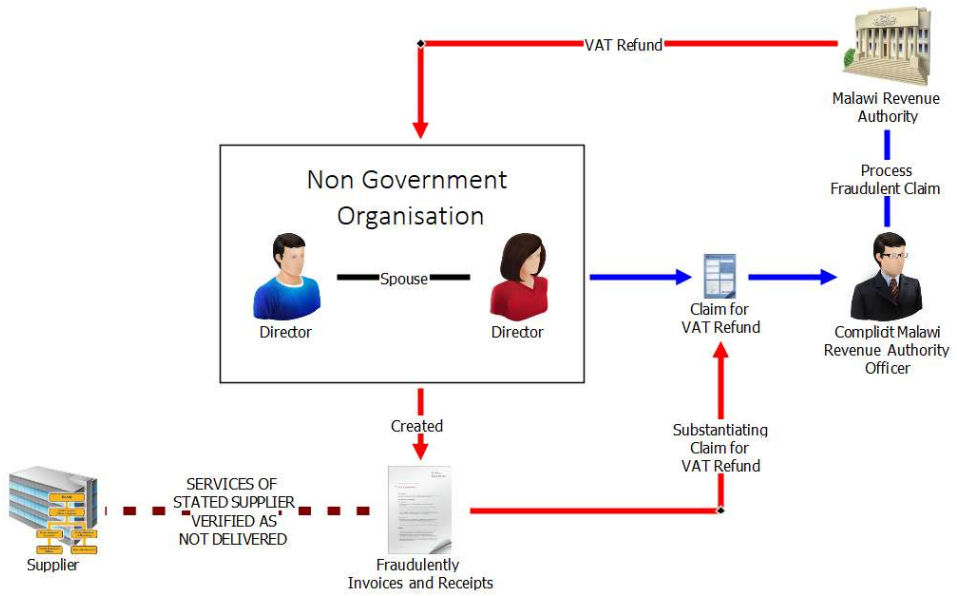
mainly by two Executive Directors of the NGO. Investigations revealed that the two directors were a couple.

Investigations noted that all the invoices used to support the VAT refund claim and the supporting receipts were falsified. An interview with the service providers alleged to have issued the invoices and receipts revealed that they did not offer the services to NGO X. Furthermore, it was established that the VAT refund claim was processed by MRA employees who circumvented controls. This was a case of collusion between the MRA employee and the NGO officials.

Subsequent action

Arrest

Criminal proceeding commenced.



Typology Visualisation-1.6.3.1A

Case Study: Falsification of VAT refund claims

Case Study 4.1.3.3: Falsification of collateral documents to obtain a bank loan.

Case description

In 2023, Lending Institution A received a loan application from person X. Person X applied for a loan amounting to MWK300 million from the lending institution. Based on the loan amount, the lending institution required that the loan should be hedged with a collateral. Person X pledged a house as a collateral for the loan by presenting a land certificate of lease from the Ministry of Lands and Housing. The Lending Institution verified the authenticity of the deed through the Ministry of Lands and Housing. It was revealed that the deed presented was falsified. The loan application was declined, and the falsified documents were confiscated.

Subsequent action

Loan application was declined

Investigations

Arrest

Case Study 4.1.3.4: Falsification of Invoices to externalise foreign currency

Case description

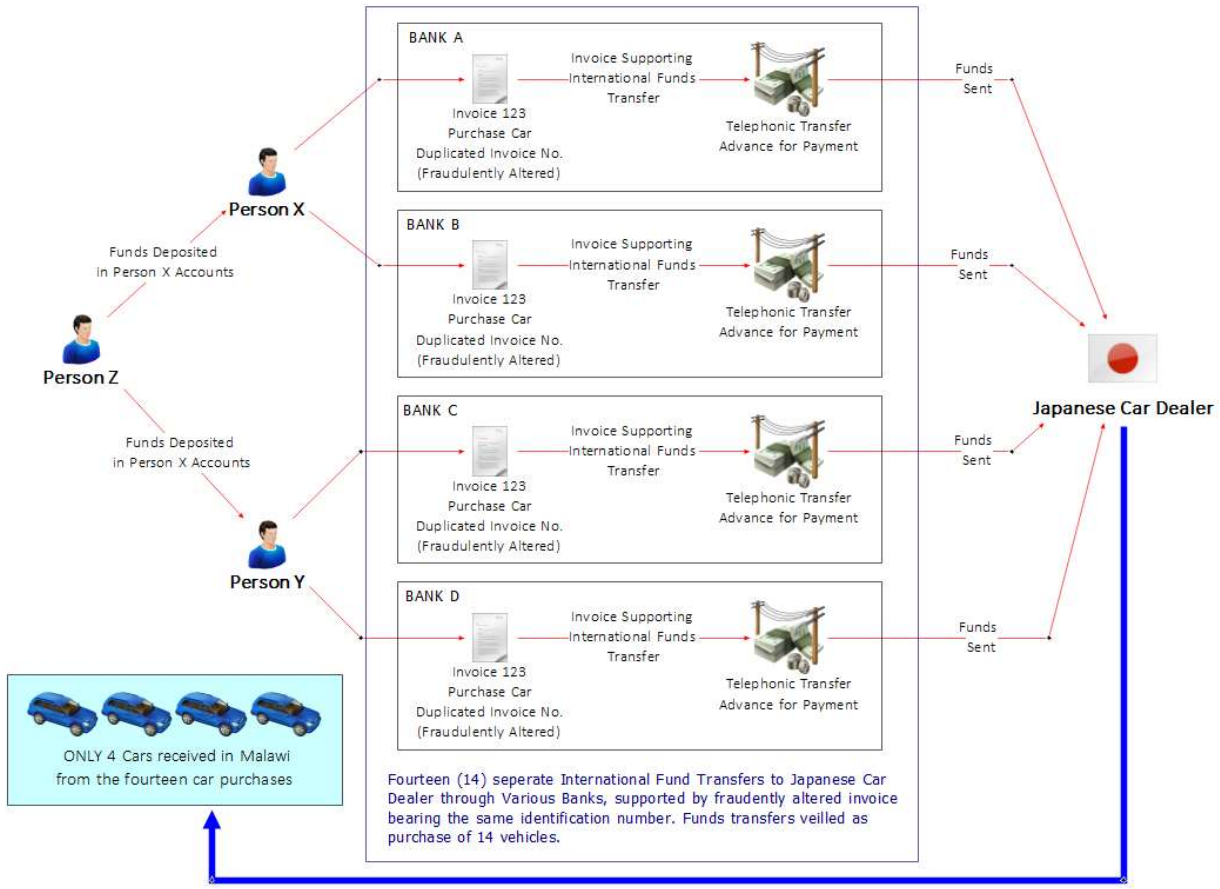
In September 2023, Bank A received a request from person X to transfer funds to a well-known second-hand car dealer based in Japan. When making the application, Person X indicated that he was purchasing a motor vehicle from the dealer. The request was supported by an invoice amounting to USD 10,000. Bank A using telegraphic transfer advanced the funds to the dealer in Japan.

In October 2023, Person Y approached bank A with request to transfer funds to the same second-hand car dealer in Japan using the same invoice totalling USD15,000. Bank A processed the request, and funds were remitted to Japan. Results of FIA analysis noted that there were 14 applications for funds transfers to Japan by person X and person Y at various banks using the same invoice.

However, in all the 14 instances, amounts and the description of the vehicles being purchased were altered on the invoice. Further analysis of bank accounts for Person X and Y noted that there was a common depositor named Person Z who was depositing funds and later externalizing them using the forged invoice. An inquiry with the MRA on the arrival of the purchased vehicles revealed that only 4 out of 14 vehicles arrived in the country. This means that funds for 10 vehicles were externalised without subsequent importation of the vehicles.

Subsequent action

Investigations, preservation of funds and dissemination to relevant LEA's.



Typology Visualisation - 1.6.3.1C

Case Study: Falsification of Invoices to externalise foreign currency

4.1.4 Typology 4: Insurance Fraud

Introduction

Insurance fraud involves any acts that are committed to defraud an insurance process with the aim of reaping monetary benefits of an insurance policy. The FIA, in its analysis, noted that there were instances whereby insurance fraud was committed, and the fraud was perpetrated by Insurance Brokers.

Case Study 4.1.4.1: Insurance fraud perpetrated by Insurance broker

Case Summary

Offences	Money Laundering, fraud and theft
Customers	Companies, Individuals
Products & services	Insurance policies
Channel	Money transfers
Indicators	• Large deposit of cash. • Overstated insurance premium. • Use of bogus insurance policy holder.

Case description

Construction Company A approached Insurance Broker X who wanted to insure its equipment. After discussions, the construction company paid insurance premium of MWK10 million through Insurance Broker X, to Insurance company Y. Insurance Broker X advised Insurance Company Y that it had to allocate MWK6 million for the equipment and that the balance of MWK4 million would be utilized by Construction Company A's employees for other insurance purposes.

Following this, Insurance Company Y started receiving some individuals purporting to be employees of Construction Company A who wanted to utilize the balance. Due to the random nature of the individuals who came to Insurance Company Y to access the balance, Insurance Company Y became suspicious and contacted the Managing Director of Construction Company A to confirm the authenticity of the employees. It turned out that all the employees who accessed the balance were not employees of Construction Company A. It was also revealed that Insurance Broker X negotiated higher premium rates with Construction Company A, but a lower rate with Insurance Company Y, resulting in over payment.

Since the Insurance Broker could not get the overpaid cash directly from Insurance Company Y, it hatched a plan of having bogus employees of the construction company to utilize the overpaid balance. In essence, the individuals who accessed the funds that were allocated as premiums for employees of Construction Company A were not for the company.

Subsequent action

Investigations.

4.1.5 Typology 5: Fraud perpetrated by Non-Governmental Organisations (NGOs)

Introduction

During the referenced period, FIA noted that some Non-Governmental Organisations (NGOs) were involved in fraud whereby their organizations were used to steal funds from the public. In Malawi, the scope of NGO's work includes developmental initiatives in agriculture, health, education and human rights advocacy, among others. The FIA noted that the victims that were affected by the fraud perpetrated by the NGOs were vulnerable people who were seeking poverty alleviation initiatives.

Case Study 4.1.5.1: AN NGO Obtaining *funds fraudulently from vulnerable people*

Case Summary

Offences	Fraud
Customers	Individual, business
Products & services	Bank accounts
Channel	Bank deposits
Indicators	• Multiple deposits in the account • Deposits followed by immediate withdrawals. • Transfer of funds to other accounts. • Abandonment of the account.
Case description In 2022, the FIA analysed a case involving NGO X. X opened a bank account with Bank B and declared that it helps vulnerable people by providing housing assistance. The NGO X identified beneficiaries for the housing project, and they demanded a processing fee of MWK 500,000 from the beneficiaries to be deposited into the NGO X's account at Bank B. Twenty-one individuals deposited their funds amounting to MWK10,500,000 as processing fee for their houses to be constructed. However, the officials disappeared with the funds. No houses were constructed for the beneficiaries, and the account was abandoned. X was a registered NGO but later X was de-registered.	
Subsequent action Investigation	

4.1.6 Typology 6: Use of New Payment Methods (NPM)

New Payment Methods (NPMs) refer to the use of the internet, wireless devices, and payment networks and does not cover the traditional payment systems of cash to send and receive money around the world. Individuals can pay or send

for goods and services using debit/credit cards, PayPal, Virtual Pay, Skrill, Ali Pay, Google Pay, Apple Pay, virtual currencies and mobile money.

These emerging payment methods accelerate cross-border, cross-currency instant, and business-to-business (B2B) payments. Due to their seamless nature, NPMs have facilitated money laundering, terrorist financing, and fraud around the world.

The NPMs will focus on the following cases:

a. Use of new payment methods to externalize and launder funds.
b. Use of Mobile Money accounts to defraud and launder funds.
c. Use of Money Value Transfer Services (MVTS) to externalise funds.

Case Study 4.1.6.1: Use of New Payment Methods to externalise and launder funds

Case Summary

Offences	Illegal externalisation of foreign currency, Money Laundering.
Customers	Individuals and Companies.
Products & services	Bank Accounts, PayPal, Skrill, Virtual Pay and POS Purchase.
Channel	Banks, Money Value Transfer Services (MVTS).
Specific Indicators	• Credits into a bank account not corresponding to the declared amount. • Transfer of huge sums in small amounts. • Rapid change in account holders' profile. • Subjects attempt to distance themselves from the transaction by creating various levels of transactions.

	• Lack of documentation for imports and sales. • Use of personal bank accounts instead of business accounts. • Operating unregistered businesses. • Prioritisation of speed over costs. • Use of vulnerable individuals to easily manipulate them in externalising or laundering the funds. • Multiple third-party cash deposits into the same account followed by outward international transfers to multiple individuals. • Narrations on the transfers made not reflecting the declared purpose of transactions.

Case Description

Malawian University Student A, worked as an agent for different foreign nationals and foreign-owned firms to externalise and launder funds. Student A opened four bank accounts (P, Q, R, and S) and declared a monthly income ranging from MWK50,000 to MWK100,000, largely from student upkeep allowances.

Soon after opening the accounts, Student A started receiving large sums of money from several foreign-owned companies and business individuals. The funds ranged from MWK1 million to MWK40 million. Within a year, two Student A's accounts P and Q received an average of MWK1.7 billion from various companies. Student A immediately transferred the funds to student B. Student A also sent MWK75 million to Student B, MWK36 million to his brother and a total of MWK31 million to two students D and E.

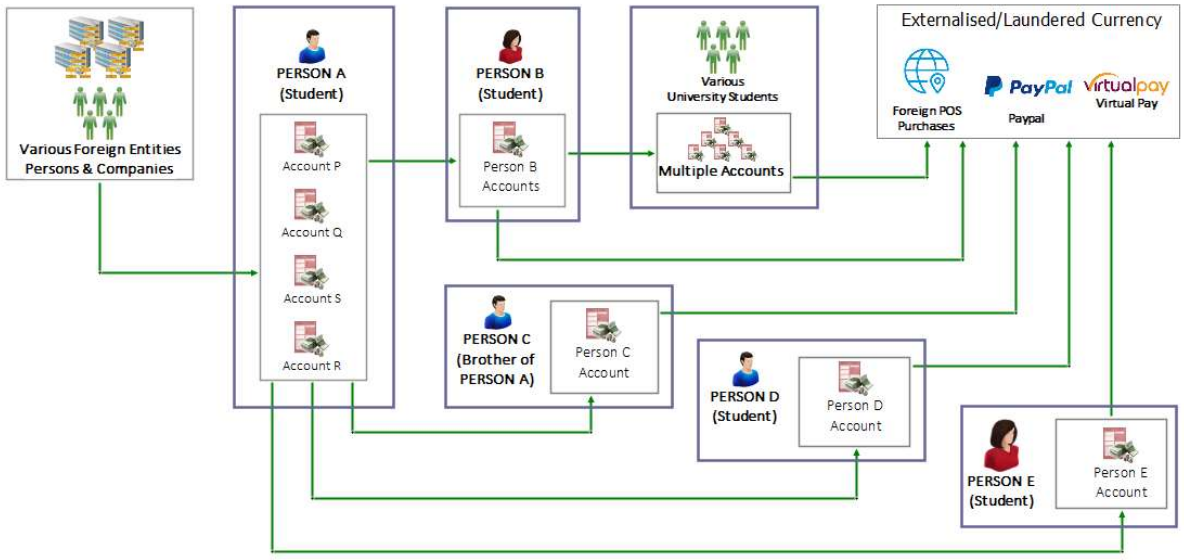
Student A tasked the female Student B to recruit other students into the scheme. Student B received MWK75 million from student A and sent MWK72 million to other students who then remitted the funds to various destinations using PayPal, Virtual Pay and POS Purchase. Student A also transferred large sums to various destinations using PayPal.

Initially, Student A alleged to run both an online electronics and farm produce business. He further stated that he purchased electronics from countries X and Y. However, in a further interview, Student A revealed that he does not have any supporting documents for either his electronics or agricultural produce business. This meant that the purported items did not arrive in Malawi, and the funds were externalised and laundered.

Further analysis indicated that Student A had transferred funds to countries other than X and Y. Student A is being used by individuals and companies to externalise funds to different countries.

Subsequent Action

Arrests and prosecution.



Typology Visualisation - 1.6.6.1

Case Study: Use of Payment methods to externalise and launder funds.

Case Study 4.1.6.2: Mobile Money Fraud

Case Summary

Offences	Fraud, obtaining money by false pretence, Money laundering.
Customer	Individuals
Products & services	Bank accounts, Mobile Money wallets
Channel	Banks, Mobile Money Operators (MMO)
Specific Indicators	• Credits into the account not corresponding to the declared amount. • Transfer of huge sums in small amounts. • Rapid change in account holders' profile. • Subjects attempt to distance themselves from the transaction by creating various levels of transactions.

	• Use of cards for a short period before adopting new cards. • Prioritisation of speed over costs.

Case Description

Mrs. A, a mobile money agent, opened five bank accounts with different banks in seven days. She linked her bank accounts with mobile platforms registered in someone else's name.

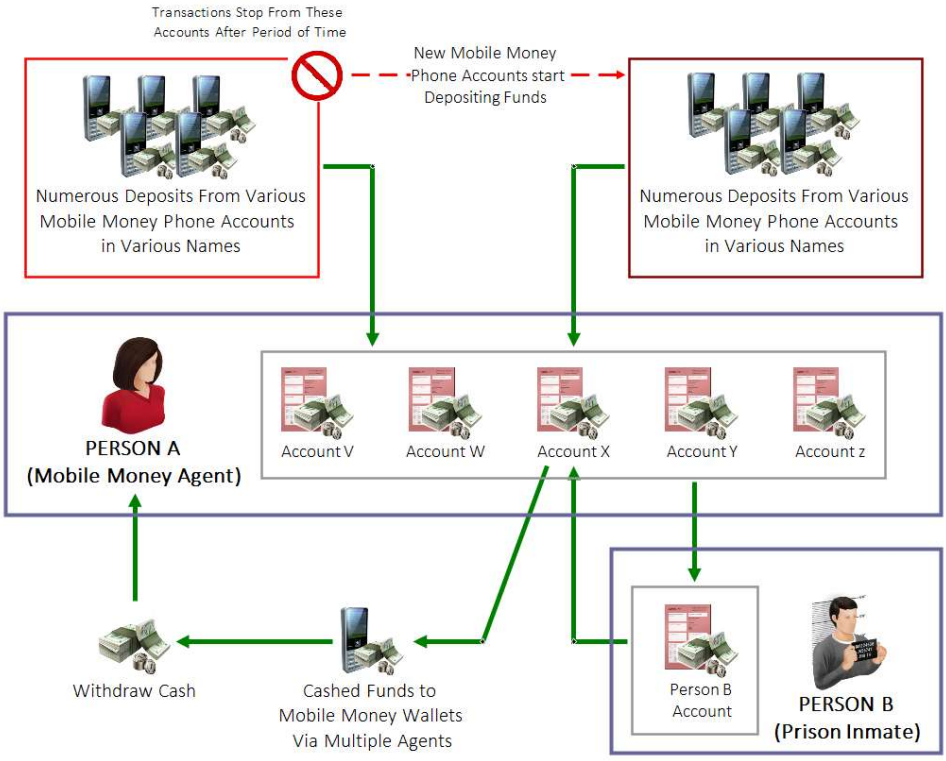
Analysis revealed that Mrs A received would defraud unsuspecting individuals, of their mobile money account funds. She later transferred the funds in different to the five bank accounts. The amounts varied between MWK50,000 and MWK1.5 million from numerous mobile money numbers for a one-year period. A set of phone numbers was used for a limited time before being abandoned and replaced with newly registered phone numbers. During the review period, MWK95 million was defrauded.

Mrs. A also transferred MWK4 million to Mr. B's bank account through an inter-bank transfer. Following the transfer, Mr. B forwarded the funds to Mrs. A's X account. Mrs. A, in turn, transferred the money to a mobile money wallet and cashed it out. The frequent transfers of funds to multiple bank and wallet accounts appeared intentional to conceal their origin.

It was established that Mr B, an inmate in one of the country's prisons, defrauded the public and transferred the funds to bank accounts owned by Mrs. A. Then Mrs. A transferred the funds to mobile money wallets before withdrawing mostly through mobile money agents.

Subsequent Action

Arrests and prosecution in progress.



Typology Visualisation - 1.6.6.2
Case Study: Mobile Money fraud and money laundering.

Case Study 4.1.6.3: Use of Money Value Transfer Services (MVTS) to externalise funds

Case Summary

Offences	Money laundering, illegal externalisation of foreign currency
Customer	Individuals
Products & services	MVTS
Channel	Money remittances
Indicators	• Multiple international remittances using third parties to the same individuals and country/destination.

	• Subjects attempt to distance themselves from the transaction by using third parties. • Multiple depositors using same KYC documentation. • Depositors profile not consistent with amounts transferred. • The frequency of deposits not making sense. • Similarity of transfer narrations and purpose. • Depositors from same location.

Case Description

The FIA received an international request from Country X to assist it with information regarding multiple remittances of funds from Malawi to two Asian national's, P and Q, residing in Country X. The remittance depositors used Money Value Transfer (MVT) Company A.

The information gathered revealed that within two weeks, numerous depositors made multiple remittances to recipient P and Q. Person P received 219 remittances totalling MWK300 million, while Person Q received 166 remittances totalling MWK250 million. The remittances to Country X were sent from the same location and in identical amounts.

Further analysis showed that several depositors used the same KYC documentation and indicated similar narrations and purposes of the funds. The depositors' profiles did not match the funds remitted.

The Persons P and Q externalized funds from Malawi to Country X by hiring multiple remittance depositors using (MVT) Company A.

Subsequent Action

Investigations, International Cooperation, report disseminated to relevant destination country.

Case Study 4.1.6.4: Impersonation to Fraudulently Obtain a Loan from a Microfinance Institution

Case summary

Offences	Attempted fraud
Customer	Individual
Products & services	Loans
Channel	Microfinance Institution
Indicators	• Unwilling to provide complete necessary documentation. • Unwilling to have institution officials visit his business premises.

Case Description

The FIA analysed a case of Customer, A of a Micro finance Institution X who applied for a loan of MWK300 million. To process the application, the Institution requested Mr. A to provide information including name, age, identity number and a passport photo of his children and spouse. However, Mr. A failed to provide the information on his spouse, instead, he brought his sister to stand in as his spouse and guarantor.

Furthermore, Mr. A did not allow the microfinance institution to visit his place of business. Based on these reasons, the institution halted the loan process because it had failed to verify the existence of Mr. A's spouse's details. The firm was afraid that it would be difficult to recover the loan in case of Mr. A's death.

It was established that Mr. A concealed information to fraudulently obtain a loan from microfinance institution X.
Subsequent Action Loan was not granted.

Case Study 4.1.6.5: Business Email Compromise (BEC)

Advancements in technology have seen an upsurge in the number of digital financial services and products including channels used to facilitate transactions. However, criminals are also using the same technology to advance their criminal activities. One of the identified criminal ways of tampering with such channels is the Business Email Compromise (BEC). BEC is a type of fraud targeting companies and individuals who conduct electronic payments. The victims are both domestic and international suppliers of goods and services. Criminals either forge the email address, send spear phishing emails or use malware to target the accounts. After they get hold of the account, they groom the target to the point that the target is convinced in sending money to unintended recipients.

The most common methods for BEC include tampering with email addresses to re-direct communication from legitimate recipients to scammers. Secondly, sending tampered documents such as emails and bank details to re-direct payments to fraudsters' bank accounts. These crimes are complex due to their transnational nature. Planning of the crime can be done in one country, execution in another and withdrawal of the funds in another.

Case Study 4.1.6.6: Theft of entity identity through email forging

Case summary

Offence	Fraud

Customer	Companies, individuals
Products and services	Bank accounts
Indicators	• Change in supplier name during the period of contract. • Subtle change of recipient details such as name, bank account number, bank, country. • Use of recipient bank account numbers that have just been opened. • Subtle changes in email addresses used to communicate very intricate matters. • Immediate withdrawal of funds using cash upon successful receipt. This makes it difficult to recover the stolen money. • Abandonment of recipient bank account after withdrawal of funds.

Case Description

In 2022, the FIA received a request to help Government Agency A in recovering funds lost through email compromise. Agency A was the implementing body for a contract to build transportation structure in the country. Furthermore, the implementation of the contract was through Company C based in Country B. In September 2018, Company D acquired Company C and adopted all the contracts that Company C had including the contract in Malawi. Therefore, the payment from Agency A was supposed to go to Company D. As a result, Company D communicated about its payment details to Agency A through emails. The payment details included bank account name and number in Country F.

In July 2019, Agency A received an email from a contact person of Company D. However, the email had a change in the address from Abcd.Defg@thehijkgroup.com to abcd.defg@thehijkgroup.com. Following this

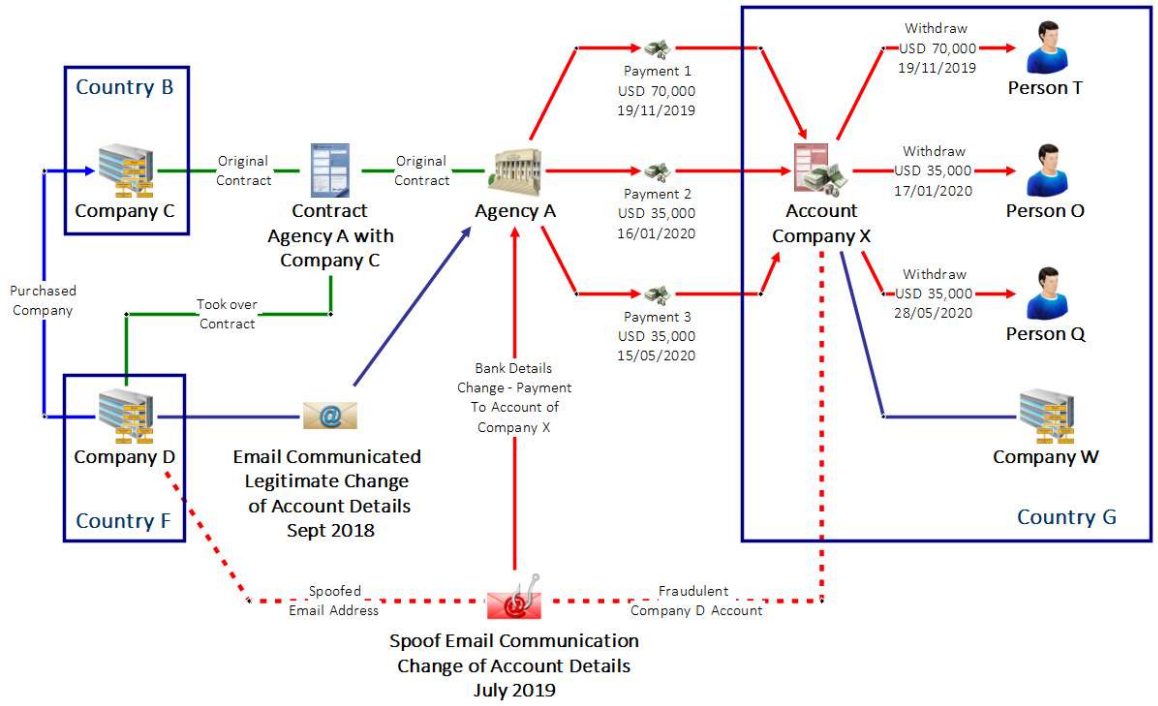
change in September 2019, Agency A received another email instructing it to send money to Company D with new account details. The new details were an account number and bank name in Country G. Between November 2019 and May 2020, Agency A made a total transfer of USD 140,000 to the new account details. The first payment of USD 70,000 to a bank account in Country G was done on 1 November 2019 belonging to Company X incorporated in that country. On the same day, Person T withdrew USD70,000. The second payment of USD35,000 was transferred on 6 January 2020 into the same account. On 15 January 2020, USD35,000 was withdrawn by Person O. The third transfer of USD35,000 was done on 16 May 2020. The funds were withdrawn on 20 May 2020 by Person Q.

Agency A noticed the anomaly in the payments in August 2020 after making the three transfers. Through international coordination, the FIA established that the transfers went into the account number and bank in Country G. However, the Company owning this bank account was not Company D but Company W. It was further noted that immediately after the bank account received the fund transfers in Country G the funds were immediately withdrawn as cash. There were three separate individuals who withdrew the cash in Country G. The main signatory to the account was not one of the individuals who withdrew the funds from the bank.

Subsequent action

Coordination with foreign counterparts.

Investigation.



Typology Visualisation - 1.6.6.5A

Case Study: Theft of entity identity through email spoofing.

Case Study 4.1.6.7: Fraud facilitated by BEC

Case summary

Offence	Fraud
Customer	Companies/individuals
Products and services	bank accounts
Indicators	• Impromptu changes to payment details from original agreement and specifications in the contract. • Unusual and subtle changes in the salient banking details. • Changes in email and IP address.

	• Discrepancy of original information and newly provided information. For example, there were notable differences with the supplier's name, postal address and physical address.

Case Description

Institution X in Malawi, got funds from Country Y to install a power station at one of its locations. Country Y identified an engineering company in Country B to offer these services. The engineering Company was Z Limited. Institution X communicated with Z Limited through email. On 30 May 2023, Institution X got an email with an invoice of GBP18,000 from Z Limited. Notably, the name of the company did not have the word "Limited" at the end. Z Limited provided its account details in Country Y.

On 11 September 2023, Institution X got another invoice amounting to GBP36,000 from Z Limited again. The details per this invoice were the exact details of an invoice from Z Limited. On 14 September 2023, Institution X instructed its bankers in Country G to transfer GBP18,000 to Z Limited. The second transfer was on 13 October 2023 of GBP36,000 to Z Limited. After these transfers, Institution X later noted that the funds were sent to a wrong account.

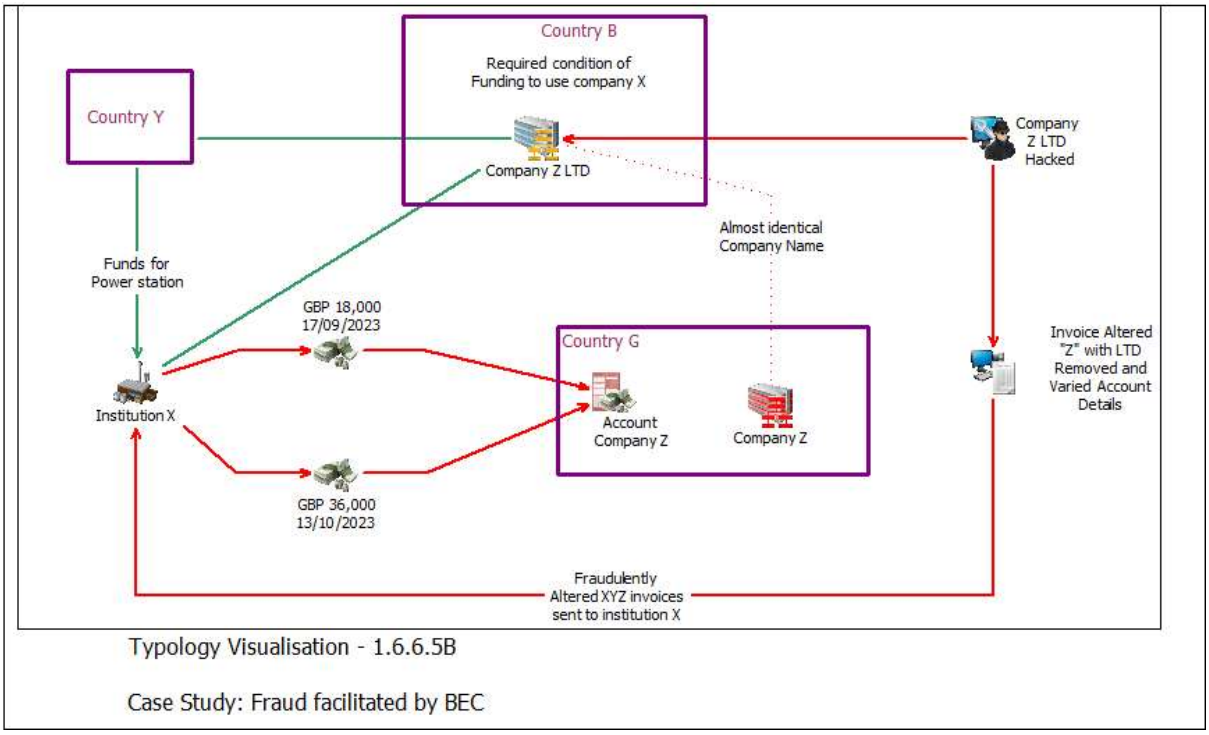
Preliminary investigation established that there was hacking into the official email of the institution. This hacking gave access to the fraudsters to edit the original invoices from Z Limited. The fraudsters changed the supplier's name which appeared the same as the original supplier. They also provided new banking details from a bank in Country G to a bank in Country X. In addition, they provided a new postal address in Country X from the postal address in Country G.

Efforts by Institution X to instruct the bank to recall the funds proved futile. The bank in Country G reported the matter to law enforcement.

Subsequent actions

Coordination with foreign counterparts.

Investigation



Typology Visualisation - 1.6.6.5B

Case Study: Fraud facilitated by BEC

4.1.7 Typology 7: Financial Institution fraud perpetrated by employees

The FIA received several STRs involving employees of financial institutions. Notably, the fraudsters targeted dormant accounts and accounts for customers residing outside Malawi. The dormant accounts were being fraudulently reactivated, and bank employees could carry out unauthorised transactions in the accounts. Funds from the accounts were then being transferred to different beneficiaries. Other fraud schemes perpetrated by employees included;

- Employees fraudulently processing cheques by flouting procedures.

- Customers depositing funds into their accounts, but the deposits not reflecting in their bank statements.
- Employees falsifying or forging procurement documents such as quotations to create a perception that the bank had legitimately procured goods.

Case Study 4.1.7.1: Bank employee transacting in the account without the customer's knowledge.

Case Summary

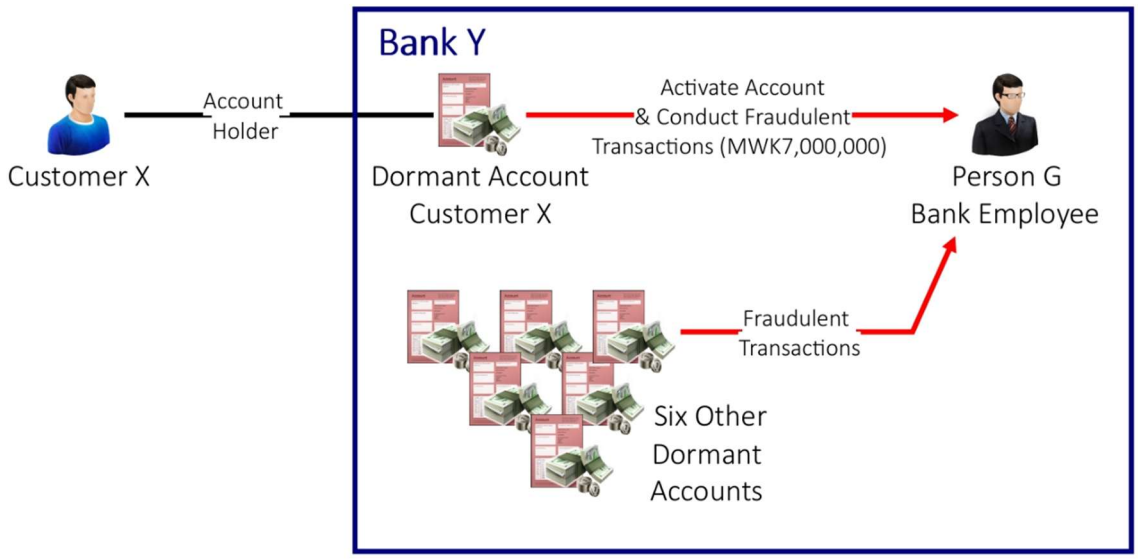
Offences	Theft, fraud, abuse of office
Customer	Individuals, entities
Products & services	Cash, bank accounts
Channels	Transfers, cash withdraws, check withdraws
Indicators	• Initiate transactions in customers' bank account without the knowledge of the owner. • Missing deposits in customer's bank statement. • Movement of funds to different e-wallet beneficiaries. • Fraudulent processing of cheques by staff through flouting cashier procedures. • Creating false procurement documents.
Case description Customer X lodged a complaint to Bank Y that there were transactions in the	

account which the customer did not initiate. The bank carried out an enquiry to validate the customer's claim. The enquiry revealed that Mr. G, a bank employee, initiated transactions in a customer's bank account after he had fraudulently reactivated a dormant customer's account. The funds debited from the account were transferred to different e-wallet beneficiaries. Investigations by the bank established that a total of MWK7,000,000 was debited from the account. It was later discovered that other six accounts were also abused by Mr. G.

Subsequent action

Mr G was suspended.

The Bank refunded the money to customer X.



Typology Visualisation - 1.6.7.1

Case Study: Bank employee transacting in the account without the customer's knowledge.

Case Study 4.1.7.2: Bank Cashier misappropriating funds

Case description
Bank XY operates a Water Board bill payment counter at one of its service centres. At the same service centre, the Water Board has its own counter which services their pre-paid customers. At close of business, a cashier for the Water Board makes a deposit of all the payments made during the day with Bank XY's Cashier. The Bank's cashier then deposits the money into the Water Board's collection account held with the Bank. On several instances, the Bank's Cashier did not credit the collection account and instead used the money for personal needs. When the Water Board officials were reconciling their account against the deposit slips maintained by their cashier, they realised that some transactions were missing and when they queried Bank XY, it was discovered that the Bank's Cashier misappropriated some deposits.
Subsequent action
The cashier was suspended and reported to Malawi Police Service (MPS).

4.1.8 Typology 8: Corruption/Bribery

Corruption is considered as the abuse of public resources or public power for personal gain. Corruption offenses, such as bribery or theft of public funds, are generally committed to gain illicit funds. Corruption and money laundering are often linked. For instance, proceeds of kickbacks and bribery are most often concealed to disguise their illegitimate source.

During the period under review, the FIA analysed reports that revealed corruption activities in the award of contracts and claim payments.

Case Study 4.1.8.1: Suspected corruption through payment claim by acquisition of land by Government institutions.

Case Summary

Offence	Corruption, Money laundering
Customer	Business/Individual
Product and services	Cheques, cash, bank accounts, and bank transfers.
Channel	Remittance
Indicators	• Account activity inconsistent with customer profile. • Cheque deposits immediately followed by transfers. • Transactions involving Politically Exposed Person (PEP). • Willingness to pay the extra charge for speedy access of funds.

Case description

The FIA analysed a report of a suspected Politically Exposed Person (PEP), Mr X who received over MWK1 billion in his personal account in less than three months from Government Institution Y. The funds were received through bankers' cheque drawn on Financial Institution Y. The cheques were cleared through cheque special clearance, a process where cheques are processed at a fee for speedy access of funds. Mr. X was a board member at Government Institution Z, which is related to Government Institution Y. Institution Y and Z operate in the same industry.

Government Institution Y confirmed paying Mr. X MWK1 billion. Institution Y stated that the payment was compensation for the land where it was carrying out its work. Institution Y stated that the initial claim was MWK10 billion, but it was

reduced to MWK1 billion after negotiating with Mr. X. Institution's Y findings on claim payment investigations did not make sense as the findings were different. Analysis showed that another individual was also compensated on the same part of the land where Mr. X received a claim payment.

Institution Y's management opted to settle the matter out of court through negotiations. No clear justification on how the initial MWK10 billion was negotiated to MWK1 billion was provided. Analysis showed that 73% of the funds received by Mr. X were transferred to his business account at Bank A and 23% of funds were transferred to his business account at Bank B. Analysis also showed that some funds were transferred to individual accounts with names like Mr. X's surname which suggested that Mr. X could be related to these individuals.

Further analysis showed that during the investigations into the claim payment, key departments such as finance were left out. The finance officers could have provided their insights on the claim payment. The finance officers were just instructed by the heads of the institution to effect, the claim payments.

Subsequent action

The report was disseminated to law enforcement for further investigations.

4.1.9 Typology 9: Tax Evasion

Tax evasion is the illegal act of deliberately avoiding paying legal taxes. Underreporting income, inflating expenses, hiding money in offshore accounts, or non-filing of tax returns are some of the ways through which tax evasion is achieved. Tax evasion consists of the element of deceit with an intended purpose of tax payment avoidance. Tax evasion is a criminal offense that can attract penalties, fines, and even imprisonment.

In Malawi, taxes include income tax, customs and excise tax on imports and exports, Pay as You Earn (PAYE), withholding tax, import duty, Value Added Tax (VAT) and export duty among others. The tax laws in Malawi require owners of businesses, both individuals and companies, to register for tax purposes regardless of the size of business, nature of business or location.

In the period under review, certain criminal trends have been noted to have made an intersection with tax evasion. One such intersection is between tax evasion and Trade Based Money Laundering (TBML), specifically through importation of goods. TBML is the process of disguising the proceeds of crime and moving value using trade transactions to legitimise their illicit origins.

Whilst in tax evasion the goal is to hide taxable income, this trend has seen the illicit income realized from tax evasion being injected back into a business as payment during import trade. Tax evasion, therefore, creates a build-up of illicit funds which are re-introduced back into the financial system through trade.

A second trend observed is tax evasion through abuse of the Value Added Tax (VAT) system. This particular tax evasion employs various methods including: issuance of fake invoices on purchases that never happened; involvement of multiple entities where goods may be passed through several countries and VAT gets claimed in all of these countries before re-exporting the goods; underreporting of sales resulting in less VAT being remitted; misclassification of goods and services to attract less VAT or as VAT exempted.

In the period under review the FIA has observed such criminal abuse of the VAT system using falsified invoices for non-existent purchases of services and goods. This trend involves collusion between taxpayers and public officers.

Case Study 4.1.9.1: Tax evasion through Trade Based Money Laundering (TBML)

Case Summary

This is a case where proceeds from tax evasion are integrated into the financial system through trade and imports, thereby creating a tax evasion-TBML cycle. In this particular case, the use of falsified invoices, non/over/under declaration of imports, multiple invoicing, non-existent transactions (no imports despite outward funds remittance), bogus suppliers are some of the methods employed by business individuals to evade tax and use the proceeds (funds that would have been remitted to the tax authority) to further their trade.

Offences	Tax evasion Trade Based Money Laundering (TBML)
Customers	Individual, business
Products & services	Bank accounts, imports, tax declarations, invoices
Channel	International Remittances
Indicators	• Using personal accounts for business imports. • Making false declarations. • Under declaration of imported good. • No evidence of imported goods arrival in the destination country. • Multiple invoicing for the same shipment. • Using fake or fictitious invoices.

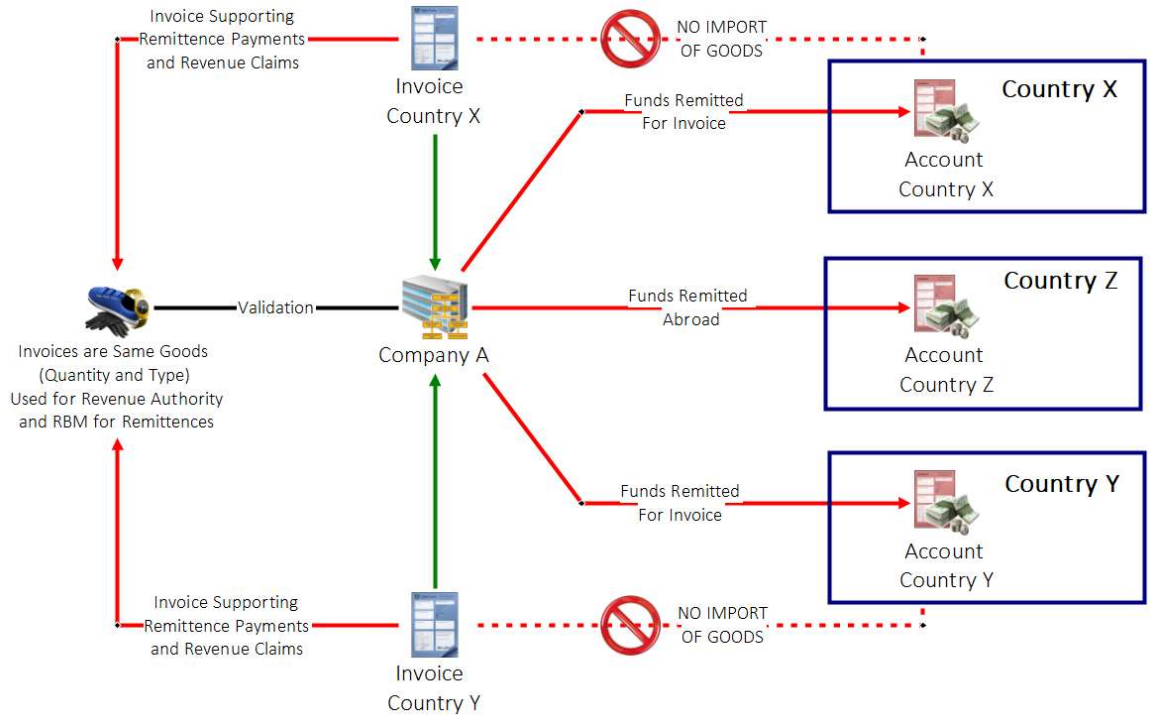
Case Description

In one of the cases that FIA analysed, the trend of tax evasion in relation to TBML was observed. A businessperson used their personal bank account to remit funds to companies in three jurisdictions for importation of goods for their business. It was noticed that some of the invoices from a company in country X, had similar banking details to that of another company in country Y. This signified falsification of invoices. Again, it was observed that invoices like the one the businessperson presented, were also presented by their relation, importing the exact same goods.

Evidence on whether all the imported goods arrived in the country was not there. In the process, there were remittances being transacted outwards with no equivalent goods being imported into the country. In addition, there were imported goods whose tax payment could not be verified, indicating under declaration to the tax authority and consequent tax evasion.

Subsequent Action

Financial and Tax investigations.



Typology Visualisation - 1.6.9.1

Case Study: Tax evasion vis-à-vis Trade Based Money Laundering

Case Study 4.1.9.2: Tax evasion through abuse of system and collusion

Case Summary

In this observed trend, an organisation colluded with a public official within the Tax Authority to make fraudulent VAT claims and get refunded for non-existent purchases of goods and services. The organisation presented fictitious VAT claims to the Tax Authority. Through manipulation of the VAT system by the public officer, the organisation managed to get unwarranted VAT refunds.

Offences	Tax evasion, fraud, bribery, money laundering.
Customer	Organisations, suppliers, public officers, NGOs.

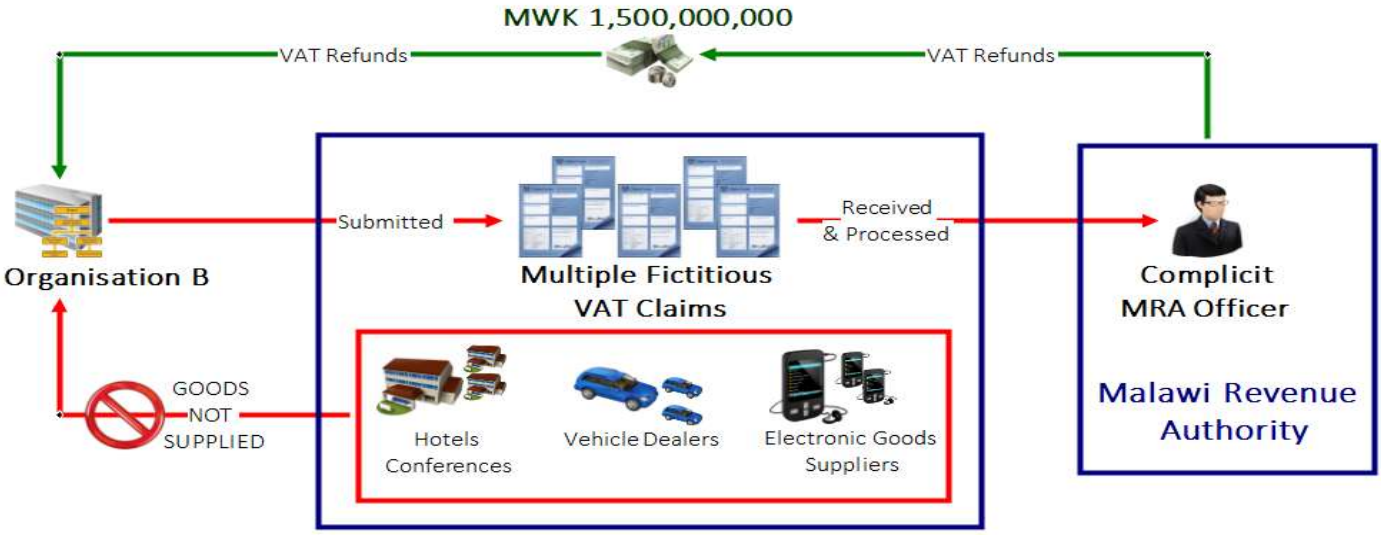
Products & services	Bank accounts, Bank Transfers, digital mobile banking platforms, VAT refund claims, invoices.
Channel	Cash withdrawals, cash deposits, digital mobile banking, bank net transfers.
Indicators	• Unusually high value VAT refund claims. • Immediate large withdrawals following account being credited with VAT refund. • High volume receipts from businesses of goods and services. • Fictitious VAT receipts from goods and service suppliers.

Case Description

The FIA analysed a case in which organisation B fraudulently claimed VAT amounting to MWK1,500,000,000 from MRA, with the help of an MRA employee. Organisation B submitted VAT claims to MRA for payments that the organisation purportedly made to goods and service providers including hotels, motor vehicle dealerships and electronic goods suppliers. It was established that none of the goods and service providers supplied any goods or services to the organisation for the material period.

Some of the fictitious indicators of the receipts presented on the claims included the following;

•Inconsistent sequence of receipt numbers. •The unusually high amount of goods claimed to have been bought (i.e. electronics). •Forged receipts and invoices of suppliers and service providers i.e hotels, lodges and hardware stores. •Taxpayer identifier for some of the suppliers was quoted wrongly on the claim receipts.
The MRA employee fraudulently examined the submitted claim receipts and signed them off as qualifying for VAT refunds.
Subsequent action Financial and Tax Investigations Arrest



Typology Visualisation - 1.6.9.2

Case Study: Tax evasion through abuse of the Value Added Tax (VAT) system and collusion with public officials.

4.2 EMERGING TRENDS

4.2.1 Typology 1: Third Party Use of Accounts

Another emerging money laundering scheme is third party use of accounts. With this trend, third parties conduct transactions in the account of someone else with an intention to use the account for fraudulent activities. In some cases, account holders act as nominees where they allow third parties to use their accounts for transactions. This may be part of an effort to hide the true ownership of funds or the transactions. Sometimes, the third parties have control of the accounts or some entities and individuals may use someone's account to transfer funds to avoid scrutiny or to evade regulatory obligations like tax. This was also observed with the abuse of foreign exchange controls, especially the use of VISA cards.

The FIA observed a trend where individuals opened accounts and immediately the accounts started receiving large deposits of funds from individuals and entities. Such deposits were commonly followed by immediate withdrawals. Notably, the magnitude of the amounts going through the accounts were not commensurate with what the customer declared when opening the account and with the nature of the declared source of income.

In some cases, criminals gained unauthorised access to an account through phishing which enabled the fraudsters to access the victims' bank details and defraud them of their funds. The criminals then transfer the funds to other platforms. The FIA noticed another practice whereby third parties used deceased persons' identification documents to transact in their account.

Case Study 4.2.1.1: Third Party use of account through transacting in deceased customer's account

Case Summary

Offence	Fraud
Customers	Business/individual
Product and services	Cheques, bank accounts and bank transfers.
Channel	Banks
Indicators	Use of a deceased person's identification
Case description Bank XYZ held an account for Mr. D who owned ABC Estate. It was claimed that Mr. D died a long time ago and the Estate was being run by his nephew Mr. B. Mr. B proceeded to apply for a trading license under the name of the late uncle. It was discovered that Mr. B had been using the bank account and a trading license in the name of his late uncle. Mr B had used the license until when the bank account was restricted for National ID update as part of KYC updates.	
Subsequent action Account blocked Customer advised to change ownership of the Estate.	

4.2.1.2 Case Study: Third Party use of Account using a Minor Account

Case Summary

Offence	Fraud, Tax Evasion
Customer	Individual
Product and services	Cash, bank accounts
Channel	Transfers, cash withdraws, cheque withdrawals.

Indicators	• Opening of a minor account. • Magnitude of transactions not commensurate with declared income. • Deposits from various individuals. • Immediate withdrawals.

Case description

Mr. Z came to Bank XY to open a minor account in the name of minor B, with MR. Z signing as a guardian to the minor. The declared source of income was indicated as parents with a monthly income of around MWK50,000.00. Bank XY observed that MR. Z had been transacting in the account from the time the account became operational because B was still a minor. Bank XY also noted that the account was receiving huge sums of money from different individuals. The amounts being transacted in the account were not commensurate with the declared monthly income. The highest deposit into the account could go up to MWK8 million per transaction.

Subsequent action

Bank XY was requested to conduct an enhanced Know Your Customer (KYC) on the account.

Investigations

Disseminated to relevant Law Enforcement Agency (LEA).

4.2.2 Typology 2: Use of Lawyers to launder proceeds of crime

Introduction

During the period under review, the FIA has come across several occasions where lawyers have been used to facilitate transfer of suspicious funds to other individuals and corporations through quick execution of court orders.

Facilitations of this nature make it hard for the country to enforce strict scrutiny of suspicious funds, and strong adherence to AML/CFT best practices.

Case Study 4.2.2.1: Unusual Transfers into a bank account

Case Summary

Offence	Fraud, Money Laundering, abuse of position
Customer	Law firm, business, individuals
Product and services	Bank accounts
Indicators	• Unusual huge one-off credit. • Irregular default judgement. • Unusual request for quick execution of court order.

Case description

Lawyer X presented to bank Y a court order to pay an amount over MWK 1.5 billion as payment to supplier Z who is said to have provided engineering consultancy services to a government agency. The defendants to the case were not given time to respond before judgement according to established civil procedure rules. The amount was later sent to Lawyer "X" bank account which was immediately frozen. A request to stay execution of the default judgement was made, and the money was returned to the Government Agency.

Subsequent action
Freezing Funds were returned to Government Agency.

4.2.3 Typology 3: De-Risking

FATF defines De-risking as a phenomenon of financial institutions terminating or restricting business relationships with clients or categories of clients to avoid, rather than manage, risk in line with the FATF's risk-based approach. De-risking can be in response to various factors such as regulatory pressure, concerns about profitability, prudential requirements, anxiety after the global financial crisis, concerns about financial crimes, and reputational risk. The financial institutions must identify, assess, and understand their money laundering and terrorist financing risks, and implement AML/CFT measures commensurate with the identified risks.

The FIA received reports from financial institutions that decided to terminate, restrict, and suspend business relationships with clients. Some of the reasons for these decisions were based on clients' noncompliance with KYC requirements, and adverse media reports including imprisonments. The financial institutions refused to enter business relationships with potential customers or terminate existing business relations with current customers.

Case Study 4.2.3.1: Business terminations and restrictions based on Non-Compliance of Know Your Customer (KYC) requirements.

Case Summary

Offence	Money laundering
Customer	Business/Individual

Product and services	Cheques, cash, bank accounts and bank transfers policy accounts, pension schemes
Channel	Remittance
Indicators	• Account activity inconsistent with customer profile. • Cheque and cash deposits followed by immediate transfers. • Cash deposits immediately followed by cash withdrawals. • Unwillingness to provide KYC documents.

Case Description

The FIA analysed reports from financial institutions on customers for non-compliance of Know Your Customer (KYC) requirements. The analysis showed that customers failed to provide KYC documents such as identification documents, proof of source of funds, proof of registration/incorporation and proof of physical address. The customers were engaged several times but did not provide the documents. Due to non-compliance of document submission, the financial institutions decided to terminate, suspend, or restrict the business relationships. They further stated that they will implement their decisions unless otherwise advised by the FIA.

The FIA advised the financial institutions that the decisions on whether to continue/not to continue the business relationship with the customers solely rested on them. On issues that focused on other regulators, the FIA referred those issues to the responsible regulators. The FIA further advised financial institutions to conduct risk assessments on their customers to identify and assess risks to make

informed decisions on whether to terminate, restrict, or suspend the business relationships with the customers.

Subsequent action

Feedback, Referral and Revision of the regulations.

Case Study 4.2.3.2: Business relationship suspension due to adverse media reports

Case Summary

Offence	Money laundering
Customer	Business/Individual
Product and services	bank accounts and policy investments
Channel	Remittance
Indicators	• Unclear KYC documents • Adverse media reports

Case Description

Mr X opened a policy account at Institution Y. The premiums amounted to MWK 15 million. Mr. X declared that the source of funds will be the company where he is one of the directors. Mr. X did not provide clear information on the nature of the business of the company declared as source of funds.

Institution Y performed an adverse media screening where it was found that Mr. X was involved in a court case involving money laundering and fraud and that Mr X was answering fraud charges in court with his client who was answering charges related to forgery, uttering false documents and money laundering charges. MWK6 billion on Mr X 's bank account was frozen for being a suspected beneficiary of proceeds of crime.

Institution Y decided to suspend Mr. X's policy pending FIA's feedback after finding out about the adverse media screening.

Institution Y was advised to carry out on boarding KYC requirements and AML/CFT risk assessment as required by the Financial Crimes Act, 2017 (FCA). The FIA advised Institution Y that a decision on whether to on board/not to on board a customer rested on them.

Subsequent Action

Institution Y did not open the account for Mr X.

Case Study 4.2.3.3: Business relationship rejected due to adverse reports

Case Summary

Offence	Theft, money laundering
Customer	Business/individual
Product and services	bank accounts
Channel	Remittance
Indicators	• Adverse reports. • Request of account opening on a recently opened company.

Case Description

The FIA analysed reports involving potential customers who wanted to open accounts at Bank Y. Before onboarding the customers, bank Y screened the customers. This was done to check if the customers had any adverse reports or not as part of customer due diligence. After screening the customers, there were adverse reports on some of the customers as follows:

Mr X

Mr X was a Malawian citizen who wanted to open an account with Bank Y in October 2023. Screening results matched him with the exact name and details of Mr. X, with adverse results. The matched individual was also a Malawian. In 2013, the matched individual was convicted in a Western country on forgery charges and for practicing medicine using a fraudulently obtained licence. The matched individual was imprisoned and deported after completion of sentence.

Analysis showed that the bank determined it was a true match after the bank officer analysed all the information provided by Mr. X. He and the matched individual had the same surname, date of birth, and nationality. Based on the findings the bank refused to open an account for Mr X.

Company X

Mr A and Mrs B, business owners of Company X visited bank Y to open a business account. Screening results on Mr. A and Mrs. B showed adverse results on similar names of Mr A and Mrs B. A result on Mr. A showed that he was a Malawian who worked in the public service. He was arrested by the Law Enforcement Agency for embezzling MWK10 million. The case was on going and that he was currently granted bail.

Results on Mrs. B showed that she was also a public servant who was arrested by Law Enforcement Agency for defrauding the Malawi government through illegal encashment of cheques to companies that did not supply goods (the cash gate scandal). Mrs. B was later charged with conspiracy to commit crime, theft, and money laundering for MWK20 million. She was sentenced to 5 years imprisonment for theft, money laundering, and fraud.

Bank Y analysed the screening results, news articles and determined that Mr A and Mrs B were true matches due to matches in names, nationalities, and addresses. Based on the findings, the bank refused to open an account for company X whose owners were Mr A and Mrs B. The FIA established that the company was recently registered by Mr. A and Mrs B in 2023, two months before visiting Bank Y to open an account.
Subsequent Action The bank rejected the account opening requests.

4.2.4 Typology 4: Terrorist Financing

Introduction

Section 43 of FCA, 2017 criminalises Terrorist Financing (TF) offence. The law provides for criminalisation of any provision or receipt of funds directly or indirectly or any attempt with an intention that the funds be used knowledgeably in part or whole to carry out a terrorist act, by a terrorist or a terrorist organization.

The law also criminalises the travel of individuals who travel to a state other than their state of residence or nationality for the purposes of the perpetration, planning or preparation of or participation in terrorist activities. During this analysis period, it was noted that TF represents a small portion of illicit transactions. The noted case study identified that there was use of mobile money services to move funds.

The TF process includes raising, moving, storing and using of funds that may either be from legitimate or illegitimate sources. The case study below identified the movement of funds by suspected UN designated grouping.

Case Study 4.2.4.1: Arrest of a sympathizer of a designated terrorist grouping

Case summary

Offence	Illegal entry, Illegal possession of firearms, TF
Customer	Individuals
Products and services	Mobile money
Indicators	• The mobile number used was not registered under the real name of the user of that mobile money account. • The money into this mobile money account passed through several channels before being credited into this mobile money account. • All transfers from the mobile money account resulted in cash withdrawals by the recipients. • Avoiding use of bank and provision of personal details to Authority.

Case Description

In January 2023, the Court in one of the districts in the country found Person A guilty of possession of firearms and ammunition without a permit. The court also found Person A guilty of illegal entry in the country. Person A is a nationality of Country X but came to Malawi through Country Y. Further investigations found that Person A is a sympathizer of Grouping B. Grouping B is designated by the United Nation Security Council as a Foreign Terrorist Organisation since the year 2004.

Person A claims that when he was in Country Y, he met people of the same religious grouping who radicalized him to be a sympathizer of Grouping B. He was, therefore, sent to Malawi to be a coordinator in implementing the

ideologies of the Grouping in Country Y that followed keenly the ideologies of Grouping B. He claimed that while in Country Y, he got money from well-wishers after distributing ideological materials via social media. When in Country Y he got money through his e- wallet. His journey to Malawi was sponsored by his colleagues in Country Y from their grouping. He entered the country illegally and had a contact person in Malawi based in District M where he got settled in October 2022. The contact person in District M was Person H. Person H is believed to be a contact person for Grouping B in Malawi.

While in District M, he settled in a village and offered the villagers some tailoring lessons. He was arrested in December 2022 after workers at a farm in the same district saw him loitering around. The workers were suspicious of his behaviour and later informed the Police. After police search, he was found in possession of firearms and ammunition, military boots and two flags belonging to Grouping B and 2 mobile gadgets. The firearms did not have a licence and he illegally possessed the ammunition. Further search in his mobile gadgets found ideological materials and texts relating to Grouping B. One mobile gadget was registered on a mobile money platform while the other was not.

The only traceable funds which he used when in Malawi were through his mobile money transaction. The mobile number was registered for mobile money services under another name, Person C. It was established that Person C is a mobile money agent and it appears he provided his National Identity to register the number of Person A on the platform. There was a direct cash transfer from another mobile money agent of MWK 120,000 on 5 December 2022. On the same day, he transferred MWK50,000 to Person M, who immediately cashed out the money. On 7 December 2022, he transferred MWK 2,000 to Person D who later withdrew the money.

Further information suggested that Person A received funds from colleagues in Country S through unknown cash courier. The money courier found an informal money changer in District M who changed the money into a local currency. Thereafter, the money was deposited with the agent who later transferred the money to Person A mobile money account.

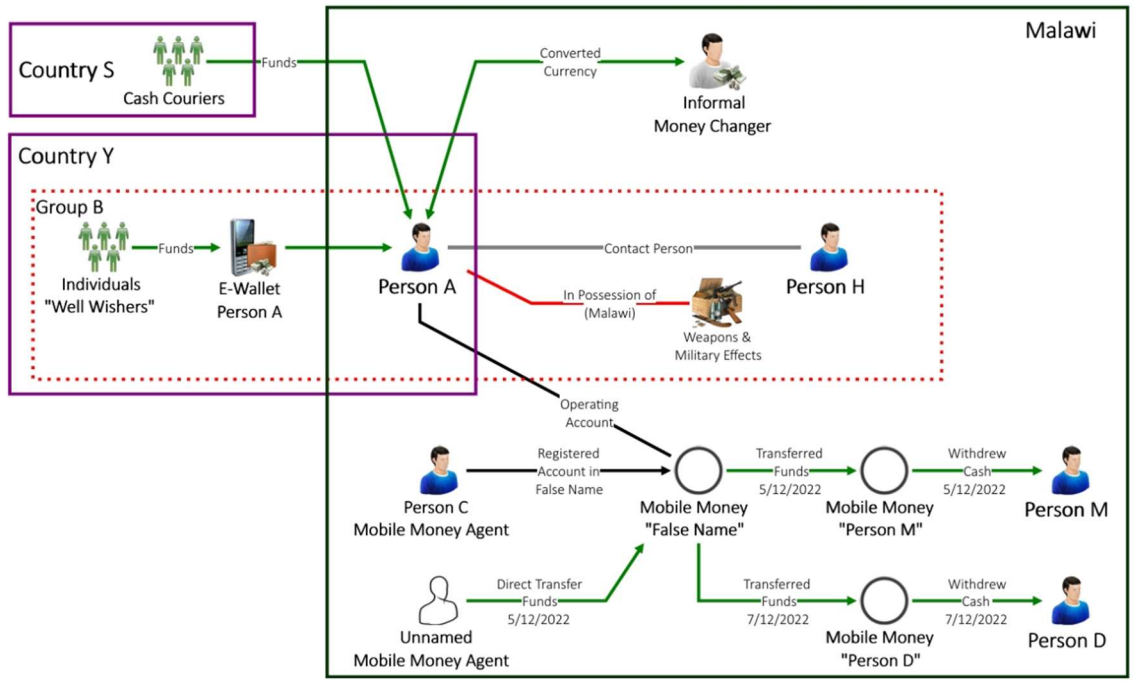
Subsequent events

Arrests

Investigations

Prosecution

International coordination



Typology Visualisation - 1.7.5.1

Case Study: Arrest of a sympathizer of a designated terrorist grouping.

4.2.5 Typology 5: Service Based Money Laundering (SBML)

Service-Based Money Laundering (SBML) is a method used by criminals to disguise the origins of illicit funds through transactions and services provided by legitimate businesses. Unlike traditional money laundering, where physical assets or cash are often involved, SBML revolves around the manipulation of services, often making it harder to detect and trace.

Case Study 4.2.5.1: Service Based Money Laundering

Case Summary

Offences	Money laundering,
Customer	Individuals, professionals, businesses
Products & services	Bank accounts, Bank Transfers, remittances, legal arrangements, investment accounts.
Channel	Remittances, bank transfers,
Indicators	• Transacting above declared income. • High volume receipts from businesses. • Non-existence of transactions related to the declared business. • Round-Tripping- Sending money to a third-party account and then having it returned in the form of a non-taxable transaction, such as a gift or loan.

CASE DESCRIPTION

The FIA analysed a case in which an individual, Mr. Y opened a business account with one of the local banks. The account received a wire transfer from country G in US Dollars. Mr. Y indicated that the funds were his payment for consultancy services that his company provided to a client in country G. However, there was no evidence of the claimed consultancy service provision. Mr. Y failed to provide proof for the source of the funds.

Once the funds hit Mr. Y's business account, there were several bank transfers to other local accounts. In addition, there were standing orders in place to have part of the funds transferred to three different jurisdictions once the funds hit the local account from country G. One notable transfer was a sum of around MK3 Billion for legal consultation to Mr. A.

Through investigations, it was established that Mr. Y never provided any consulting services warranting the remittance from country G. Again, the legal services that Mr. A purportedly provided to Mr. Y were vague and could not be accounted for.

Consequently, the funds in Mr. Y's business account, and that in Mr. A's account were frozen and preserved for forfeiture.

Subsequent action

Financial investigations, assets preservation

4.3 ASSET RECOVERY EFFORTS

As part of its efforts of fighting financial crimes, the FIA is part of the task force on asset recovery. It plays a big role to ensure that illicit gotten assets are confiscated and forfeited to the State. The FIA is at the centre of using Non-Conviction-Based Forfeiture (NCBF) under the Financial Crimes Act. During the period under review the FIA managed to recover assets.

The FIA got two preservation orders of MWK43.4 million in accounts belonging to civil servants on 5 October 2022 in (Civil Cause No. 317 of 2022). Funds amounting to MWK 1.535 billion in a Construction contractor vs Government Agency case were forfeited on 30th March 2023.

In July 2022, the FIA got a court order on forfeiture of MWK12.3million in *Civil Cause Number 58 of 2022*. This was a case of illegal externalization of foreign currency and money laundering through mobile money virtual cards. At the period end, there were three cases before the courts for conclusion of forfeiture processes with amounts of MWK113,102,195.00, MWK11,353,516.03 and MWK158,097,965.00.

For more progress to take place for asset recovery, there is need for continued capacity building in asset tracing, financial data analysis and financial investigations. Additionally, there is need to ensure adequate staffing and funding of Law enforcement agencies to improve operational capacity.

5 RECOMMENDATIONS

5.1.1 Improving the Foreign Currency Exchange legal and regulatory framework

The legal and regulatory framework regarding foreign currency exchange should be strengthened. There should be efficiency in enforcing the laws such that offenses should be penalised. The mandatory requirement of exporters to

repatriate proceeds of export sales should be adhered to. There should be proper mechanisms in place to ensure that this is being done. In addition, there should be deliberate efforts to promote use of official foreign currency exchange platforms and remove the use of parallel exchange markets.

5.1.2 Prevention of theft by public servants

- Authorities should ensure that there are collaborative efforts by all relevant authorities to implement preventative measures against theft of public funds. These measures should be enhanced by advances in Information Technology. Digitalization of work processes will enhance efficiency, transparency, and accountability in public financial management.
- In addition, inter-agency collaboration should be promoted to ensure success in the fight of financial crimes. These include the Financial Intelligence Authority (FIA), Anti-Corruption Bureau (ACB), the Malawi Revenue Authority (MRA), the Office of Director of Public Officers' Declaration (ODPOD), Office of the Director of Public Prosecutions (DPP), and the Malawi Police Service (MPS), among others.
- There should be increased efforts in asset recovery by relevant stakeholders.

5.1.3 AML/CFT/CPF Controls

- Reporting institutions should pay attention to different red flags by adopting transaction monitoring systems.
- Mobile money operators should review their SIM card registration policy and implement strict KYC procedures to prevent fraud.
- Financial institutions should conduct proper customer due diligence to verify the identity of customers and assess the risks associated with them.

- Financial institutions should conduct enhanced due diligence to scrutinise higher-risk customers or transactions. There should be ongoing monitoring to frequently check on customer transactions and customer activities.
- Financial Institutions should implement a Risk-Based Approach to De-Risking. Before de-risking, a thorough risk assessment of each customer or group of customers should be conducted to ably make informed decision.
- Financial institutions should have proper procedures (clear ways of communicating with different customers) when providing awareness to customers on KYC updates.
- Financial Institutions should have proper policies and procedures on how to deal with clients with non-compliance issues and those customers with adverse media reports.
- Regulators should help guide non-compliance challenges faced by financial institutions and, where possible provide general guidelines on the same.

5.1.4 Enhanced Due Diligence on Transactions and Customers

- Financial institutions ought to put extra effort in verifying existence and authenticity of suppliers before conducting the transactions.
- Efforts to create a better understanding of TBML.

5.1.5 Prevention of online payment fraud

- Entities should ensure segregation of duties when it comes to payment processes originating from emails. There should be a process of review to scrutinize payment details and ensure that funds are transferred to intended recipients or beneficiaries.

- There should be a proper examination of email address, URL and spellings used in correspondence before a payment is executed.
- There should be thorough scrutiny of documents and circumstances surrounding payments of such magnitude.
- There should be use of encrypted emails, with two-way authentication.
- Verify payment details and invoices through making a phone call or virtual meetings to ensure that the details are legitimate before making final payment instructions.

5.1.6 Screening of reporting entity employees

Reporting entities should ensure that employees are properly screened before handling customers bank accounts. On controls, proper reviews and monitoring of controls should routinely take place to ensure that they are efficient. Proper policies should be put in place to ensure that employees do not face financial pressure to compel them to steal from customers or the entity as this may tarnish the reputation of the reporting entity.

5.1.7 Prevention of procurement fraud

- Strengthen payment controls and monitoring to ensuring that claims are verified, matched with contracts, and supported by adequate documentation before disbursement.

- Implement strong internal controls and oversight mechanisms to enforce segregation of duties within procurement, finance, and contract management processes to ensure that no single individual has control over multiple steps.

- Regular internal and external audits of procurement and payment processes should be conducted. This will help to identify and address irregularities and ensure compliance with policies.
- Develop and enforce specific policies to prevent, detect, deter and respond to false claims and bribery in contract awards.
- Encourage whistleblowing and protect whistleblowers. This will help individuals to report any corrupt related activities.
- Regulators should help guide non-compliance challenges faced by financial institutions and, where possible provide general guidelines on the same.

5.1.8 Responses to TF

- Strengthening border controls to ensure travellers enter the country legally.
- Regulators in the mobile money sector to ensure there are policies preventing registration of mobile money accounts by using third party identification documents.
- Ensure prosecution of TF offence under the Financial Crimes Act (FCA), 2017
- Improved coordination amongst relevant domestic stakeholders in investigations and prosecutions of TF cases.
- Increased capacity building in TF amongst all relevant stakeholders.

5.1.9 Public awareness

- There should be deliberate efforts to create a greater understanding of ML/TF/PF methods and techniques.

5.1.10 Public Private Partnership

- There should be efforts to establish public private partnerships to establish and promote awareness between reporting entities.
- Exchange of information on emerging risks such as crypto currency.