MONEY LAUNDERING TRENDS AND TYPOLOGIES REPORT

FINANCIAL INTELLIGENCE AUTHORITY

With a vision for a financial crime-free Malawi

Abbreviations and acronyms

Abbreviation	Meaning
AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorism
CDD	Customer Due Diligence
FATF	Financial Action Task Force
FCA	Financial Crimes Act
FIA	Financial Intelligence Authority - Malawi
MLCO	Money Laundering Compliance Officer
PEP	Politically Exposed Person
STR	Suspicious Transaction Report
ESAAMLG	Eastern and Southern Africa Anti- Money Laundering Group
EGMONT	Group of FIUs
KYC	Know Your Customer
LEA	Law Enforcement Agency
ML/FT	Money Laundering/ Terrorist Financing

1. Introduction

The Financial Intelligence Authority (FIA) is established by section 3 of the Financial Crimes Act No. 14 of 2017 (FCA) as Malawi's national central agency responsible for combating money laundering, terrorist financing and the proliferation of weapons of mass destruction.

The core functions of the FIA are to receive and analyse financial transaction reports from financial institutions and other reporting entities and to disseminate financial intelligence to law enforcement agencies and other relevant stakeholders for further investigation. The FCA gives the FIA additional powers which include, among other things, the power to conduct parallel financial investigations and to restrain, recover and manage the proceeds of crime.

The FIA continues to work with various stakeholders locally and internationally in combating money laundering and terrorist financing. Within the local framework, the FIA works closely with the Malawi Police Service (MPS), Anti-Corruption Bureau (ACB), Malawi Revenue Authority (MRA), Department of National Parks and Wildlife (DNPW) and the Reserve Bank of Malawi (RBM) amongst other relevant stakeholders. These stakeholders are the main recipients of our financial intelligence. Further, the relationship is multidimensional in that the FIA receives and analyses information from reporting entities as well as requests for information from stakeholders. The FIA is also a member of several taskforces set up to achieve specific goals in combating financial crime such as wildlife, exchange control violations and the sharing of information.

Internationally, the FIA is a member of the Egmont Group of Financial Intelligence Units. The Egmont Group is an informal network of FIUs around the world with a current membership of over 150. The Egmont Group provides a platform for the secure exchange of expertise and financial intelligence to combat money laundering and terrorist financing (ML/TF). Malawi is also a member of ESAAMLG, a regional FATF-style body. The FIA participates in ESAAMLG activities by demonstrating excellence in information sharing/exchange through the ESAAMLG FIU Forum.

The above connections make the FIA uniquely positioned to produce strategic intelligence reports such as this Trends and Typologies report. Such reports allow for stakeholders to understand and enhance defence mechanisms to ensure Malawi meets the global Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) standards laid down by the FATF.

1.1 Objective

This report primarily addresses the reporting institutions and Law Enforcement Agencies (LEAs) on the emerging and continuing escalation of some typologies in money laundering happening in Malawi. The public is also appraised on how criminals are using the financial system and the mechanisms they employ to launder the proceeds of crime.

It is worthwhile for the FIA to produce strategic intelligence reports such as this report to ensure the active participation of reporting entities, LEAs and the public in combating ML/TF. This report contains sanitised cases (case studies) that provide insights into those that are charged with various roles and responsibilities in combating, investigating and prosecuting financial crime. Members of the public are further made aware of the techniques that criminals are employing so that they can avoid becoming victims or being used as conduits that may cost them up to a lifetime of imprisonment.

1.2 Executive Summary

The 2017/18 Trends & Typologies report covers a number of areas such as wildlife/environmental crimes, theft of public funds and abuse of office, concealing assets/funds by circumventing customer identification requirements and the use of nominees, obtaining funds under false pretences, money laundering through illegal externalisation of foreign currency and insurance disinvestments. This report also focuses on the proceeds derived from the above predicate crimes.

Malawi has seen an increase in reported environmental crimes relating to fauna and flora. The courts have convicted several suspects and meted out various degrees of punishment to the perpetrators, ranging from fines to imprisonment. The FIA has been instrumental in assisting LEAs with financial analyses and reaching out to foreign jurisdictions within the Egmont Group or under bilateral arrangements. However, the fight against wildlife crime is facing a number of challenges. There is an urgent need for prosecutors and investigators of wildlife crime to consider following the proceeds of this crime. This can be achieved through multi-agency cooperation and tying money laundering charges together with the predicate crime.

Since 2016, various stakeholders have come together under the umbrella of an inter-agency network/taskforce fighting wildlife crime. The taskforce consists of the FIA, MRA, DPP, MPS, ACB and DNPW and others. The taskforce has registered some success, but this needs to be further strengthened by ensuring that the proceeds of crime are taken away through an asset forfeiture regime. In all cases that have been tried in court, only one case has resulted in a money laundering conviction. Other cases are still being tried with money laundering charges attached.

The FIA has not received any Suspicious Transaction Reports (STR) on the subject, as most of the work has been done as a result of requests from other agencies. It should be noted that STRs on environmental crimes have not been forthcoming, as case studies have shown that the individuals involved usually use cash and not the traditional financial system for their transactions. Very few transactions go through money remittance services disguised as payment for legitimate exports/imports.

It has been nearly five years since the first Cash-gate cases were unearthed. There has been a further onslaught on public funds through other means by unscrupulous officers. Just like Cash-gate, some officers are using loopholes in the public financial system and exploiting them for their own benefit. Unlike in the 2015-2017 Trends and Typologies report, the perpetrators have identified new techniques to launder their ill-gotten proceeds. This report outlines these methods in detail. It is worth noting that the FIA is working with stakeholders to bring the vice to a halt. In the previous reports, the FIA concentrated on the emerging trends around predicate crimes.

In this edition, the FIA through the STRs it has analysed has noticed an emerging trend whereby some individuals circumvent customer identification requirements to conceal the beneficial owner of funds. We have come across people using third parties to open accounts that are used to receive fraudulent funds transfers. Ultimately the individuals control the account without the knowledge of the alleged owner (the third party) of the account. Financial institutions are responsible for instituting preventative measures against customers that would use their products and services to conceal illicit funds through know your customer (KYC) or Customer Due Diligence (CDD) requirements. Despite having these measures some customers still try to conceal the beneficial ownership of the funds that are in the financial institution.

The FIA has further noticed an emerging trend in the insurance sector where typical investment portfolios are subsequently disinvested for reasons that do not make economic sense within a very short period of time. The trend mostly involves individuals rather than legal persons. Usually the investment is made in cash and upon disinvestment, the funds are payable in the form of an instrument or a transfer that may appear to legitimise the source of funds once the funds hit the customer's account at the recipient bank. It should be noted that the cases studies under this category have not been tested and concluded. However, the cases show tell-tale signs of irregular and illegitimate financial activity with the aim of laundering the proceeds of crime. Insurance companies are urged to fully implement KYC measures at the on-boarding stage and during the course of the business relationship and report attempted or unusual transactions that follow this pattern.

2. Overview of the STRs Received

This section looks at the general overview of the STRs received from the reporting institutions, which were analysed and/or disseminated to LEAs. The aim of the section is to provide feedback to the reporting institutions to help them in strengthening their AML compliance regime and particularly to identify and file STRs.

The report covers STRs that were received and analysed from the various reporting institutions for the fiscal year 2017/2018 (July 2017 to June 2018). Great focus has been given to reports from banks, as banks continue to be the source of most of the STRs that are analysed and disseminated to LEAs. 91 STRs were received, of which 81 were from the banking sector and 8 from the insurance sector.

2.1 General Observations on the STRs Received

2.1.1 Common/prevalent indicators

- Large cash deposits remain a prevalent indicator. Personal bank accounts being credited regularly with huge sums of cash where there is no known business and source of income. We noted, however, that most customers do not truthfully declare their sources of income, hence lots of legitimate transactions are reported as STRs.
- Forged and false documents used to apply for foreign exchange. This follows large cash deposits with immediate applications for foreign exchange. The forged documents include invoices, export documents, travel documents and cheques.
- Large sums of cash deposits from multiple sources into a newly opened account followed by immediate international transfer/application for forex purchase.
- Opening of parallel accounts with the aim of diverting funds intended for the main account, particularly cheques, to the parallel account. For instance, employees opening a parallel account for an institution's welfare program and depositing cheques written in the name of the institution's account, and meant for the genuine account, into the parallel account.
- Providing false account opening details and false business financial statements with the aim of defrauding the bank through accessing loans.
- Under-declaration on KYC in terms of expected turnover and source of income. Lack of enhanced CDD by the financial institution resulting in the filing of STRs where updating of KYC information could have resolved the suspicions.
- Use of third parties and nominees. The use of third parties like relatives and associates to receive suspicious funds from the proceeds of a financial crime.
- Financial institutions honouring instructions made electronically without verifying the authenticity of the messages.

- Multiple customers involved in different types of businesses but who appear related conducting international funds transfers to the same overseas beneficiary.
- Unreported cases or a lack of transaction monitoring mechanisms. Due to challenges in transaction monitoring, some suspicious transactions are never noted and subsequently not reported.
- Sale of large sums of foreign currency whose source is unclear or disguised as proceeds from the sale of farm produce across Malawi's borders.
- Account activity inconsistent with a customer's profile. For instance, a young person who is still serving public office receiving a pension even when they have not reached retirement age.
- Customer unwilling to provide further information when requested to by a financial institution and terminating the business relationship. This has been common in the insurance sector.
- Customer providing falsified financial account to obtain a loan, credit or overdraft facility from a financial institution.

2.2 Recommended and Possible Sources and Triggers for STRs

2.2.1 Public/media information

The FIA notes that other suspicious transactions are left unreported due to challenges with transaction monitoring and the failure to use public information on possible financial crimes. For instance, information on people arrested for financial crimes like corruption, fraud and wildlife crimes can help to trigger suspicions where transactions are made in accounts of the concerned persons and their associates. Reporting institutions need to use widely available information to check their clientele against adverse news, either from open or closed sources.

2.2.2 Conduct and actions of employees of financial institutions

Whilst there has not been a concluded case relating to breaches in financial institutions, there are instances of wilful negligence where staff have overlooked policies and procedures. There have been incidents where employees have connived with suspects to defraud other customers or the financial institutions. Some staff have been in contempt of banking procedures and have been assisting customers to easily access certain products and services that have stringent requirements in contravention of some laws. The relevant authorities must take the initiative to prosecute and penalise negligent employees or those who wilfully aid and abet the malpractice.

2.3 Emerging Risks

2.3.1 Trade-based money laundering

These are cases of over-invoicing and forged invoices used with a bid to externalise funds. In most cases, there is a mismatch between the known business turnover and the amounts being externalised. For example, a small trading shop or business in salt that regularly eternalises funds under the guise of importing machinery.

2.3.2 Illegal trade in wildlife and wildlife products

Accounts benefiting from the international inward transfer of funds from destinations associated with the ivory trade and drug trafficking.

2.3.3 Mingling of legitimate and illicit funds

This refers to the mixing of illegitimate funds (proceeds of crime) with those from a legitimate business. The launderer has a front business that he uses to introduce dirty money into the financial system, usually at the placement stage.

2.3.4 Identity theft

This ranges from forged identification documents to tampering with communication lines, whereby fraudsters get access to victims' phone numbers and use them to confirm or request fraudulent payments.

2.4 Challenges Related to Filed STRs

2.4.1 Use of shell companies and comingling of legitimate and illicit funds

It is hard to prove the true sources of funds when suspects hide behind a legitimate cash-intensive business and mingle this income with proceeds from crime and illegitimate business dealings, e.g. ivory trade, sales from illegal logging, black forex market.

2.4.2 Use of nominees and third parties

Lawyers and accountants provide services that can be used to conceal the origin of money, such as purchasing property, securities and other investment assets on behalf of their customers. This is extended to customers who act on behalf of others to transact in the financial system.

3. Money Laundering Methods and Techniques

The FIA reviewed and analysed the STRs and requests received in 2017/2018, from which it has observed emerging and ongoing money laundering methods and techniques. In this report, the FIA notes that wildlife crime is posing a major threat to several wildlife species in Malawi. The major species heavily threatened in Malawi are elephants hunted for their ivory, and mukula and cider trees used for logs. There have been a number of seizures of ivory in Asia and Australia of ivory consignments originating from Malawi. Malawi is both a source of and transit country for illegal wildlife products. The FIA has specifically observed some trends and techniques used when moving the illicit proceeds of the illegal wildlife trade in Malawi.

3.1 Preference for remittance transactions to move illegal proceeds

- International money/wire transfers from jurisdictions with a high risk of wildlife crime to suspected wildlife crime syndicates in Malawi;
- Transfers from jurisdictions with a high risk of wildlife crime to people in the freight forwarding business in Malawi;
- Transfers from high-risk jurisdictions to companies in Malawi suspected of being involved in wildlife crimes. This has been unearthed through a mismatch between the economic activity and the money remittance received;
- Other indicators include foreign nationals purportedly hiding behind legitimate businesses as fronts for the illegal wildlife trade.

3.2 Use of third parties to receive and transfer the illegal proceeds and conceal properties obtained from the proceeds of crime

- Corrupt public officials use family members, third parties and associates to launder the proceeds of crime and conceal the true ownership of funds and assets;
- Relations of public officers are being used to launder illicit funds by carrying out transactions and purchasing property on behalf of corrupt officials;
- Properties/real estate registered in the names of family members to distance themselves from illicit funds and avoid detection from authorities.

3.3 Providing false information to meet customer identification requirements

- Mostly common in trade-based money laundering. Concealing information about the beneficial owner or control of funds to hide the link between funds involved in the transaction and the criminal act from where the funds were generated;
- Creating an impression that the transaction is legitimate when it may raise suspicions if the correct information is provided;
- Use of fake business registration certificates, fake identities and fake import documents.

3.4 Collusion between employees of reporting entities and crime syndicates to circumvent transaction requirements

- Trade-based money laundering is a growing concern in the banking sector with the growth in international trade. ML is facilitated by collusion between importers, exporters and bank officials, who are given an inducement to execute the illegal transactions;
- Bank officials process import payments by ignoring Exchange Control Regulations i.e. allow import payments without supporting documents;
- Bank officials process import payments without carrying out enhanced customer due diligence of the sender and beneficiaries.

3.5 Disinvestments of insurance policies

- Customers deliberately refuse to meet identification requirements, forcing insurance companies to cancel policies. When such funds are reimbursed by the insurance company (by cheque/transfer), the launderer has successfully obscured the link between the crime and the generated funds;
- Early redemption as an indicator of money laundering occurs when the potential policyholder is more interested in the cancellation terms of a policy than the benefits of the policy. The launderer buys a policy with illicit funds and then informs the insurance company that he has changed his mind and cancels the policy, agreeing to pay the penalty.

4. Money Laundering Typologies in Malawi

4.1 Typology 1: Environmental crime and the use of remittances to move illegal proceeds

In 2017, the FIA noted an emerging trend in which suspected syndicates involved in wildlife crimes had been receiving funds suspected to be proceeds from wildlife crime. The syndicates received the funds through Western Union and international transfers disguised as upkeep and investment capital. The funds were broken down into smaller transactions which added up to huge amounts but were received in amounts ranging from US$5,000 to US$50,000. The origin of most of these funds was Hong Kong.

These funds had been received by the suspects after several suspected illegal shipments of government trophies (wildlife parts and products) from Malawi had been intercepted in Singapore, Thailand, China and Australia.

Case summary

Offence	Illegal possession, dealing in government trophies
Customer	Individuals
Products	Remittance services and cash
Indicators	International funds transfers from foreign nationals and jurisdictions which do not make business sense

4.1.1 Case study 1.1: Transfers from high-risk jurisdictions to mining companies in Malawi suspected of being involved in wildlife crimes

In 2017, there was an interception of 422 pieces of ivory weighing 330 kg in an Asian country. The ivory originated from Malawi. Local investigations established that the ivory was shipped by a foreign national in collusion with freight forwarding companies and LEA officers at one of the international airports in Malawi. The consignment, which was declared as rough stones and packed in 15 cartons, weighed about 2 tonnes. The authorities arrested 7 suspects, including one foreign national who was the main principal suspect.

Further investigation established that the main suspect has a registered small mining company and was also an employee of another mining company involved in rough stones. Around the same period of the shipment, there was an inflow of funds amounting to US$50,000 from Hong Kong to the mining company, whose purpose was indicated as investment capital.

However, the flow of funds did not make economic sense since there was no known link between the directors of the mining company where the main suspect worked and the origin of the funds. It is highly likely that the funds were part of financial flows of illicit proceeds from wildlife crime in which the mining company is involved. It is believed that the mining operation was a front for the illicit trade in government trophies, in this case ivory.

Indicators and red flags

- Mismatch between the economic activity, country of origin or person and the money remittance received;
- International funds transfer receipts not tallying with declared business;
- Unverified financial capital investments from other jurisdictions;
- Collusion between exporter and local officials to circumvent pre-shipment inspection at the port of exit.

4.1.2 Case study 1.2: Transfers from jurisdictions with a high risk of wildlife crime to suspected wildlife crime syndicates in Malawi

In 2013, two Malawians were arrested after being found in possession of 781 pieces of ivory weighing 2,640 kg and valued at about US$6 million (MK4.3 billion). The ivory was concealed in a consignment of bags of cement. The ivory was coming from Tanzania, transiting Malawi and destined for Mozambique. The pair were charged with the offences of possession of specimens of protected species and money laundering. They were convicted and ordered to pay a fine of US$7,000 (MK5 million) or face five years' imprisonment. There was information that the two Malawians were part of a syndicate of foreign nationals who were not identified and arrested.

The FIA noted that one of the two convicted individuals received funds from Hong Kong through Western Union. Hong Kong and China are known to be destinations for wildlife products. There was no mutually beneficial legal economic activity connecting the origin and beneficiary of the funds. The only likely explanation for the link was that the funds were payments for the wildlife products, considering that the recipient was part of a syndicate involved in wildlife crime in Malawi.

Indicators and red flags

- International funds transfer receipts not tallying with declared business;
- Unverifiable connection between originator and beneficiary of international funds transfers;
- Concealment of illegal items or contraband in regular imports.

4.2 Typology 2: Theft of public funds

During the period under review, the FIA established a scheme and emerging trends in the abuse and theft of public funds, particularly pension funds. Due to a lack of checks and balances and to laxity in transaction monitoring in the pension payments systems, some officers tampered with the system and managed to insert ghost pensioners on the pension payroll. This was overpaying some pensioners by figures that were over 500% in some cases.

The involvement of third parties in the system delinked the individuals that compiled the beneficiary list and those that uploaded the list for pension payments via the government system. This created an opportunity for government officers to insert names and tamper with the figures.

The payment system at commercial banks, which depends on correct account numbers and not names, created an opportunity for the diversion of funds to the accounts of the officers on the basis of valid account numbers despite using fake/ghost account names. Public officials used third parties to receive and transfer the illegal proceeds and also to conceal properties obtained from the proceeds of the

Case summary

Offence	Theft by public officers
Customer	Public officers
Product	Transfers and instructions
Services	Accounts (Savings and Current)
Channel	ATM, money transfers, face to face
Indicators	Monthly pensions credits Third parties Irregular government payments

4.2.1 Case study 2.1: Abuse of office and theft

The pensions payments division entrusted Public Officer X to assist with the uploading and encryption of lists of names of pension beneficiaries to be sent to individual commercial banks for payment. Officer X became the liaison point between the payments office and the commercial banks.

In and around July 2016, Officer X tampered with the list from the payments office and added ghost names to the list. The ghost names were directly connected to Officer X's personal bank accounts and a joint account he held with his spouse. Other names were linked to his acquaintance, Mr. Y. The account details of the ghost names bore legitimate bank account details belonging to Officer X and his acquaintance Mr. Y, who has never worked in government.

Officer X took advantage of loopholes in the banks' payment systems, which rely on verified account numbers and do not cross-check with account names in order to carry out payments. From the ghost names, X syphoned off huge sums from July 2016 to March 2018.

When the authorities discovered the scheme, Officer X was arrested and charged with the offences of theft by a public servant and money laundering. In money laundering terms, Officer X used the proceeds from the crime for living expenses and to purchase a house and two undeveloped residential plots.

Indicators and red flags

- KYC Information on Age: The suspected pension beneficiary is a young man whose age is way below the government retirement age;
- Third parties (ghost beneficiaries) transferring funds to the public officer: Legitimate pension funds were credited to bank accounts of the suspect's relatives and associates, who in turn were getting a commission and transferring the funds to the suspect's account;
- Mismatch of information: Account names of the ghost pensioners did not match the names at the bank, although the account numbers were legitimate. The accounts belonged to the suspect and his associates.
- Dubious amounts: Based on public information on the levels and expected public servant's salaries and pensions.

4.3 Typology 3: Trade Based Money Laundering (TBML) - Collusion between importers and bank officials to avoid customer identification requirements and allow illegal transactions

The FIA has observed that trade-based money laundering remains a major threat. Unlike in the previous report, where legitimate businesses were used to illegally externalise foreign currency through import payments supported by fake MRA Form 12 documents, there is an emerging trend whereby importers and some personnel of financial institutions collude to avoid customer identification requirements and allow illegal transactions. Some importers have used fake business registration documents to open bank accounts. The fake business registration certificates enable the beneficial owners of the accounts to be hidden. The fictitious businesses made huge import payments.

In 2017, the FIA uncovered a scheme whereby foreign exchange transactions amounting to about US$6.4 million (MK4.7 billion) had been conducted by fictitious businesses whose beneficial owners could not be identified. In addition, close to US$6.8 million (MK5 billion) was externalised through transactions without supporting documents. This was made possible through collusion between the businesses involved and the employees of the financial institutions concerned.

Case summary

Offence	Submitting false documents, money laundering, illegal externalisation of foreign currency, tax evasion, corruption
Customer	Sole proprietors, partnerships
Products	Wire transfers, cash deposits, cheque deposits
Indicators	False declarations, fake business registrations, frequent wire transfers, missing importation documents, sudden enrichment

4.3.1 Case study 3.1: Providing false business documents to make transactions legitimate.

Between July and August 2017, FIA carried out investigations on four Pakistani nationals who used seven businesses to externalise US$6.4 million (MK4.7 billion) to about three beneficiaries the in United Arab Emirates, China and India in a period of 6 months (January to July 2017). To make the transactions appear legitimate, the foreign nationals provided false information. They provided false business registration certificates and made false declarations indicating that they were importing packaging machines.

The results of the investigations showed that business registration certificates for the business were fake, as they were not found in the database of the Registrar of Companies. The declarations showed the importation of machines but no machines were imported.

The foreign nationals were arrested and are currently being tried in court for money laundering and contravention of Exchange Control regulations.

Indicators and red flags

- Frequent use of foreign currency for import payments;
- Use of false business licence certificates and import documents;
- Use of one business premises by a number of businesses (sharing same physical address);
- Type of business not commensurate with account turnover.

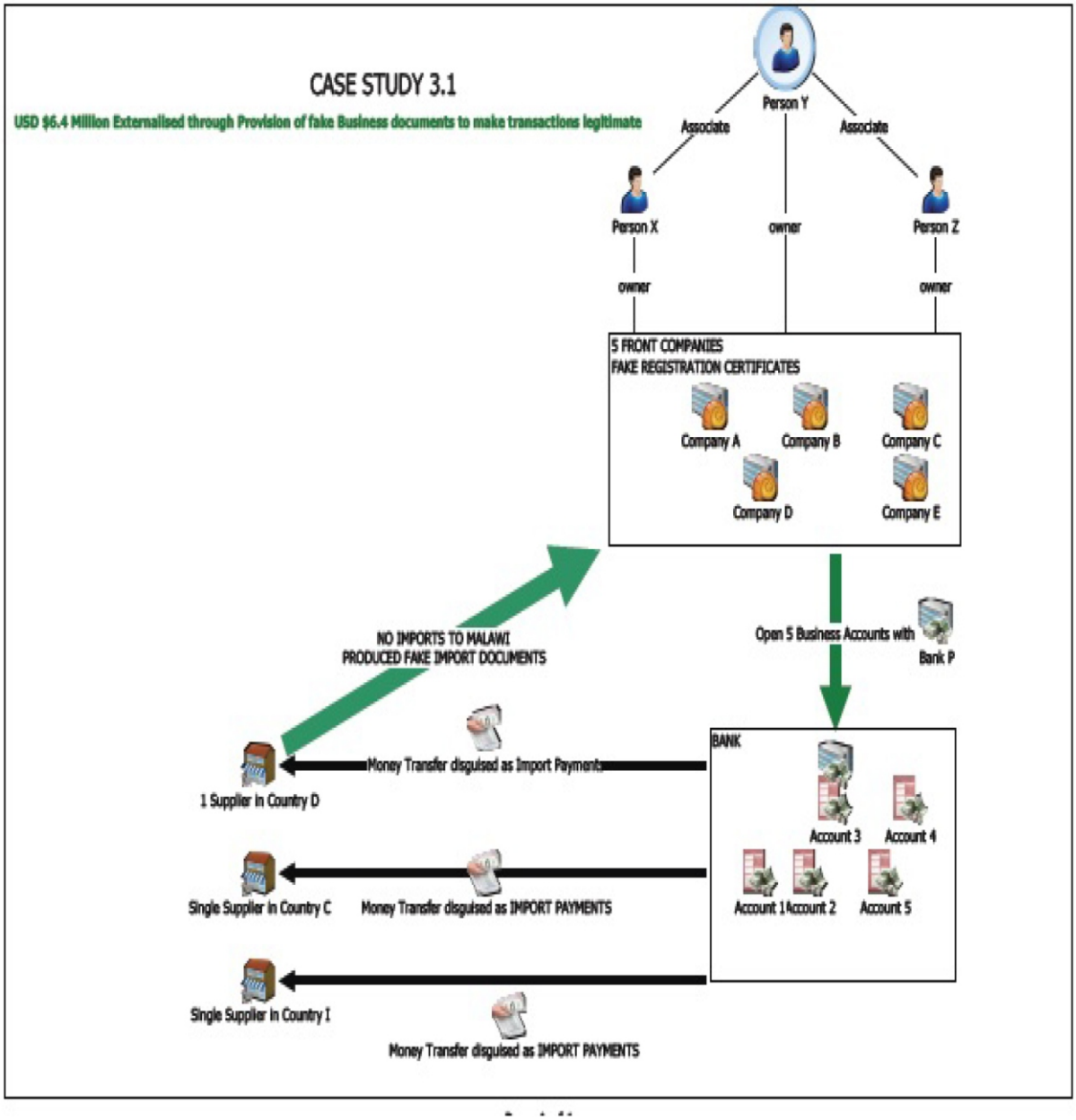


Figure 1: Case study 3.1

4.3.2 Case study 3.2: Collusion between importers and bank officials to allow illegal transactions

Around December 2017, the FIA investigated over 10 businesses owned by Chinese nationals who together externalised US$6.8 million (MK5 billion) in over 40 transactions in a period of four months (January to May 2017) through Financial Institution X. The Authority further established that there were no documents supporting the international remittances and Financial Institution X stated that the documents were missing. The transactions were not reported to the Reserve Bank of Malawi as required under the Foreign Exchange Regulations. Since there are no supporting documents, it was not possible to ascertain the purpose of the transactions or the origin and ultimate destination of the funds, let alone the ultimate beneficiary. The investigations established that the transactions were conducted by at least three officers in Financial Institution X.

Further investigations show that during the period of conducting the transactions, Officer Y, who was one of the officers who conducted the transactions, had suspicious huge cash deposits in his account suspected to be from the importers with whom the officer connived to externalise funds without supporting documentation. For example, in the period January to March 2017, Officer Y made cash deposits into his account amounting to about MK140 million. This was also the period when the funds were externalised without supporting documents. The cash deposits were not commensurate with Officer Y's known sources of funds. Officer Y eventually stopped working with the financial institution. Comparatively, three months after stopping work (April-June 2017) Officer Y only made MK3 million in cash deposits. The significant drop in cash deposits may explain that the huge cash deposits during the period of employment may have been bribes for facilitating international transfers without supporting documents.

Indicators and red flags

- Frequent use of foreign currency for import payments;
- Collusion between customer and bank official to facilitate illegal transactions;
- Lack of supporting documents for foreign exchange transactions;
- Foreign exchange transactions not reported to RBM as per requirements;
- Sudden enrichment by bank official (unexplained wealth).

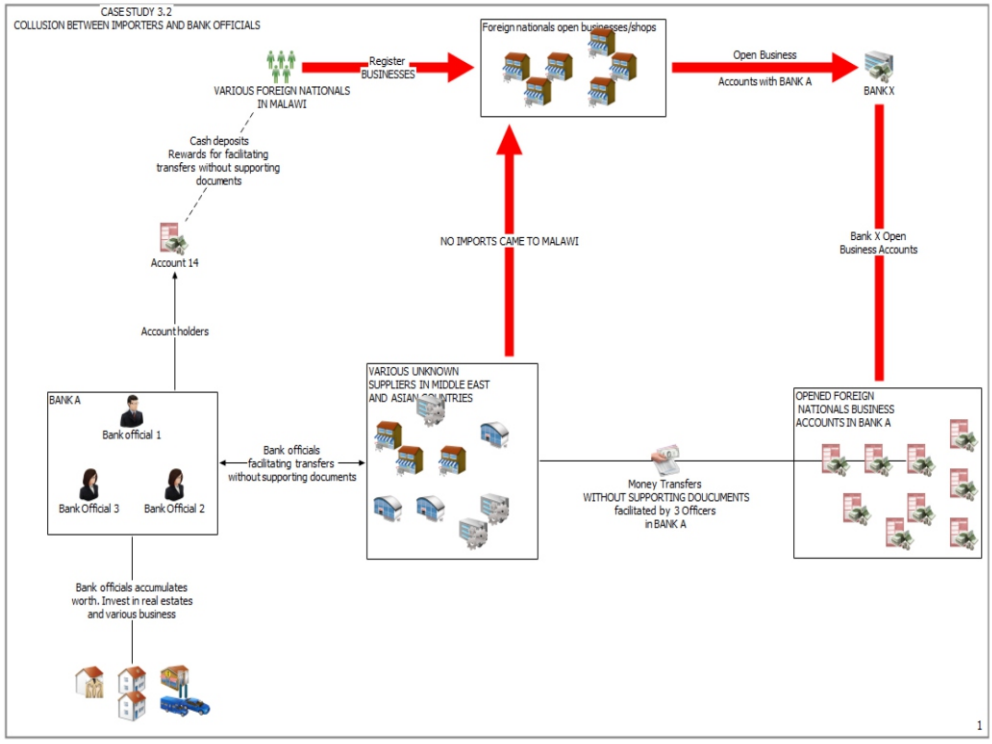


Figure 2: Case study 3.2

4.4 Typology 4: Insurance - Disinvestments of insurance policies which do not make economic sense

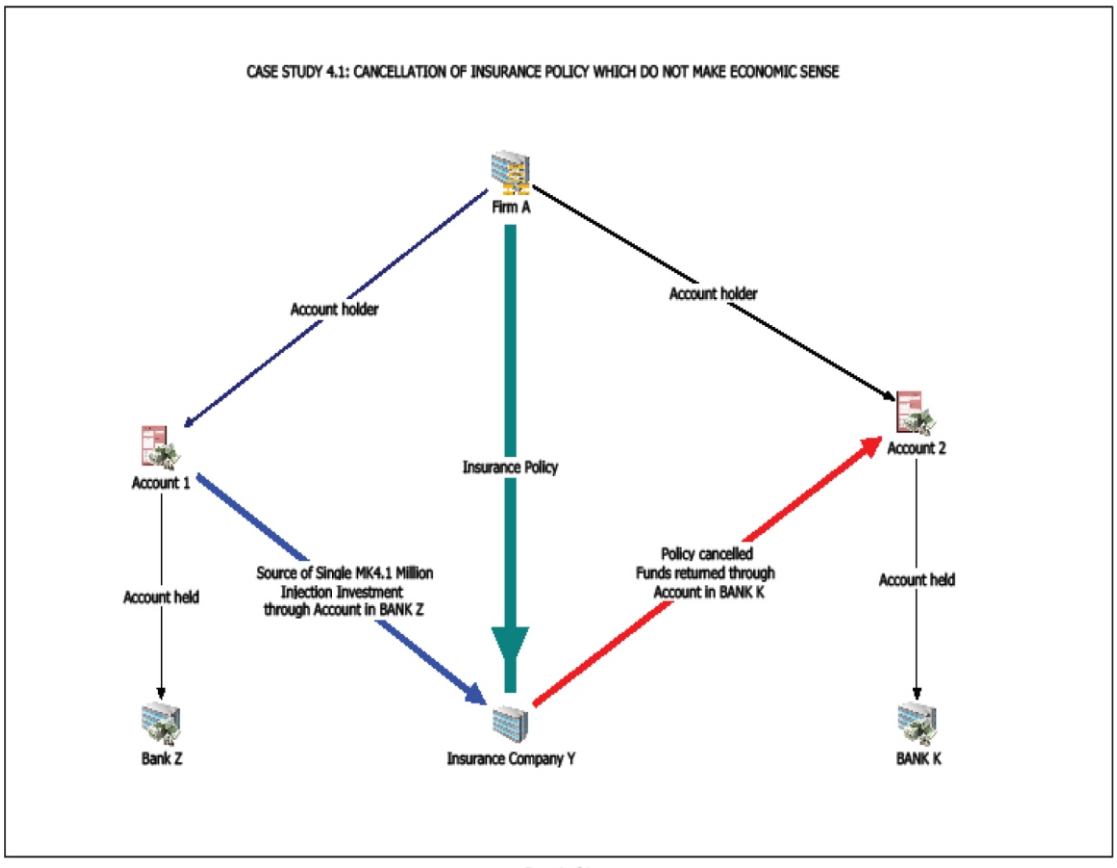
The FIA has uncovered a trend whereby customers deliberately refuse to meet identification requirements, forcing insurance companies to cancel policies. When such funds are reimbursed by the insurance company (by cheque for example), the customer will have successfully obscured the link between the crime and the generated funds. It is under these circumstances that the customer moves the funds from the beneficiary bank to other financial institutions, purportedly as clean funds.

4.4.1 Case study 4.1: Cancellation of policy after refusal to meet KYC requirements and requesting return of premium credited to an account different from the original account

In 2017, officers of Firm A made a premium injection of MK4.1 million into Insurance Company Y on behalf of their firm. The investment was made through two cheques from the firm's account in Bank Z. After about two months, Insurance Company Y requested additional KYC documents from Firm A. The KYC documents requested included audited financial reports and the instruction of signing arrangements. However, on receipt of the request, Firm A wrote to Insurance Company Y requesting cancellation of the policy and the return of the invested funds. A further instruction was that the funds be returned through another of Firm A's accounts in Bank K, despite the funds coming from its account in Bank Z. The cancellation of the policy and return of the premium to a different account were highly likely carried out to launder funds.

Indicators and red flags

- Customer reluctance to fulfil KYC requirements;
- Customer cancellation of policy regardless of penalty;
- Customer insistence to use a different account to received proceeds from early cancellation of policy.



4.4.2 Case study 4.2: Early redemption of insurance policy used to launder funds

Early redemption as an indicator of money laundering happens when a potential customer is more interested in the cancellation terms than the benefits of the policy. The customer buys a policy with illicit funds and then informs the insurance company that he has changed his mind and cancels the policy, agreeing to pay the penalty. The customer redeems the seemingly clean cheque from the insurer.

In December 2016, Person X made two premium injections of MK15 million into Insurance Company Q. Both payments were in cash. The reasons for the investment were not indicated. The proof of the source of funds was suspicious, though indicated as the sale of property.

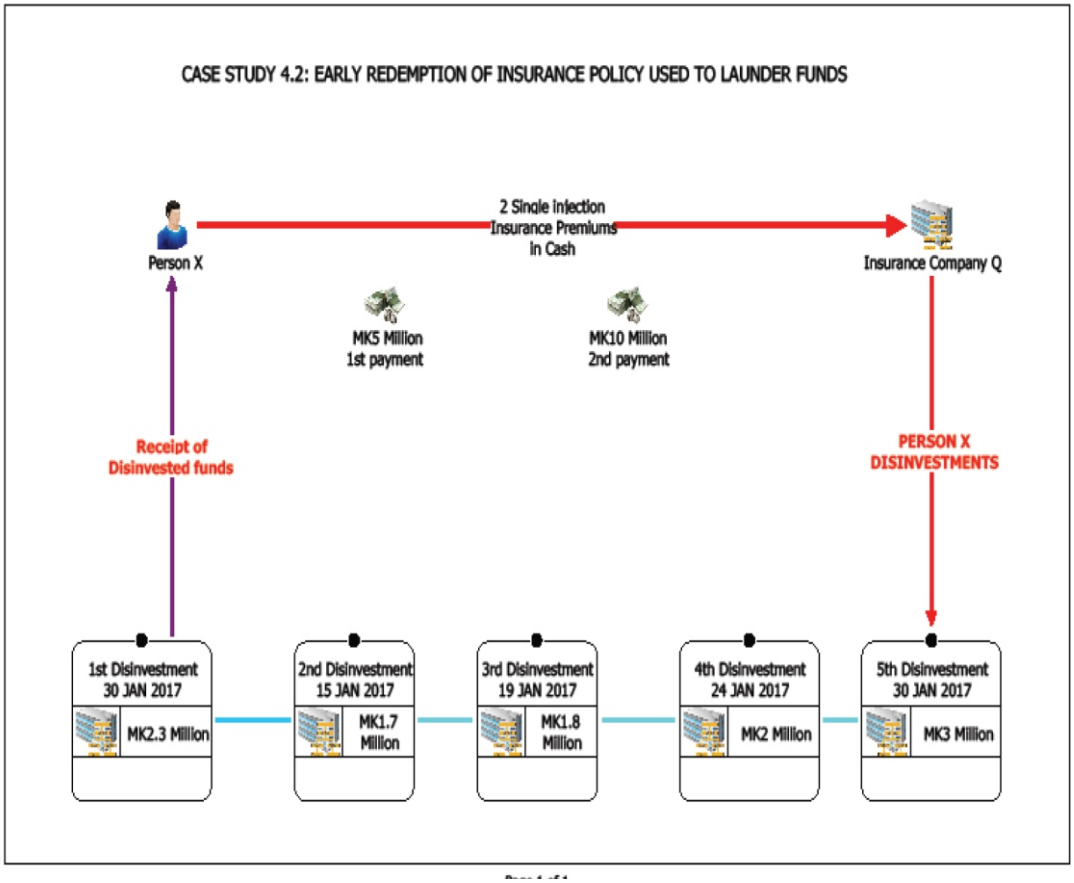
In January 2017, after only about a month, Person X started disinvesting the funds.

- First disinvestment on 5 January 2017 - MK2.3 million - reason: business investment;
- Second disinvestment on 15 January 2017 - MK1.7 million - reason: business investment;
- Third disinvestment on 19 January 2017 - MK1.8 million - reason: again, business investment;
- Fourth disinvestment on 24 January 2017 - MK2 million - reason: maintenance of business building;
- Last disinvestment on 30 January 2017 - MK3 million - reason: household expenses.

The early redemption and the manner in which it was done raised suspicion that the initial investment was made to launder funds which could have been proceeds of crime. Person X was later discovered to be connected to the plundering of public funds.

Indicators and red flags

- Customer disinvestment of investment within a short period of time;
- Large cash deposits as investment (source of funds unverified);
- Customer willing to pay penalties for early policy cancellation;
- Customer purportedly disinvesting a long-term investment to pay for regular expenses.



4.5 Typology 5: Concealing Beneficial Owner of Bank Account

4.5.1 Case study 5.1: Channelling illicit funds via a domestic worker's account

S was a senior official of a financial institution and purportedly assisted his domestic worker to open a bank account. The domestic worker, K, was to become an unknowing victim of a money laundering scheme.

The scheme worked in a very simple manner. S had recommended to his domestic worker to open the account to receive and access his monthly wages and possibly save some money for a rainy day. S then took control of the account and fraudulently diverted millions of kwachas from the financial institution's (his employer's) accounts to K's account, which he had assumed control of after having registered via internet banking and other remote services on the account. S would then transfer the funds into his account.

Between 2016 and 2017, S transferred MK29 million into K's account. The deposits were followed by an immediate transfer into his own account. It is believed that some of the funds were invested in real estate and other movable assets. Additional information revealed that S transferred some funds into an investment vehicle at one of the investment companies. S was already a subject in FIA's database from his dealings with the bank and the investment companies.

The suspect was arrested and the case is currently being handled by one of the LEAs.

Indicators and red flags

- Use of third parties;
- Simplified KYC not commensurate with account activity;
- Use of non-face-to-face products and services.

In another related case, a foreign national B assisted an acquaintance to open a business bank account. Due to language barriers between the bank official and the acquaintance, it was B who actually completed the account opening forms and was operating the account. Without the knowledge and consent of the acquaintance, B used the account to externalise funds.

Indicators and red flags

- Customer receiving funds transfers from unrelated parties;
- Sudden and unexplained enrichment by an official;
- Simplified or low KYC account transacting above threshold;
- Use of non-face-to-face products and services.

4.6 Typology 6: Use of falsified financial account/statements, shell companies and company structures

4.6.1 Case study 6.1: Using false financial statements to obtain loans

An agricultural commodities company CM was registered in Malawi in 2010. The company was involved in the buying, processing and exporting of commodity H.

The company's shares were split between two families. Peculiar to the shareholding structure is that the principals, M and Y, deliberately distanced themselves from ownership and control. Their roles were only loosely connected to the company's dealings.

The company had been applying for seasonal facilities from different financial institutions since 2012 using false or fraudulent financial statements. The company defrauded five commercial banks; the total amount swindled by the company for the period 2013 to 2016 was about US$15 million. The loans were purportedly obtained to buy/assist farmers to produce cotton on a large scale.

The defrauded banks were presented with different financial statements for the same years. The statements demonstrated a healthy company and were used to obtain the loans. Despite receiving the loans, the company did not use the money for the intended purpose. Some of the funds were kited within the banking sector in a Ponzi scheme to clear other loans that had fallen due. Some funds were transferred outside the jurisdiction through a number of ways including hawala.

Stocks for commodity H were used as collateral for the loans. A collateral manager (company) was contracted to take care of commodity H and produce period reports on commodity H bought, processed and sold. It is believed that the collateral manager conspired with CM to defraud the financial institutions with false quantities of commodity H bought and produced. The falsified reports were much higher than the actual quantities bought. It is, however, not known at what level the collateral manager was involved in the fraud.

After the loans were drawn down, they were deposited into the company's various bank accounts with different banks. These deposits were followed by huge cash withdrawals. It is believed that the money was illegally externalised to Dubai, India, Pakistan and other countries. One of the directors, Y, a suspect in the case, also travelled extensively to the said jurisdictions, among others.

Additionally, some of the money was transferred to different bank accounts owned by CM and other related companies. Thereafter some transfers were made to Hong Kong and Singapore. Despite these payments being made, there is no proof that any goods were brought in Malawi or services rendered as a result of these transfers.

Some alleged exports were traced to a company in the United Arab Emirates. A search of the company and owners led to an individual from Eastern Europe with a background of money laundering using similar techniques of obtaining loans and fleeing. Further, a company with a similar name to CM was established by Y in one of the financial centres in Europe.
There followed a joint investigation in which several people were arrested and are currently on bail. The suspects are currently in court for the US$5 million they fraudulently obtained from one of the financial institutions.

Indicators and red flags

- Obscure company ownership and control. The persons of interest created a layer of anonymity around how they operated the company. Their names were appearing as owners of the business but they were signatories to the company bank account;
- Unverified financial statements. Use of falsified financial accounts to dupe banks into thinking that the company was healthy;
- Large loans not commensurate with known business. The loans obtained did not match the numbers in the proceeds of exports;
- Lack of use of credit reference agencies;
- Use of dubious email addresses for instructions and confirmation of payments from other jurisdictions.

5. Recommendations

This section sets out a number of recommendations that Malawi should follow in order to combat and prevent money laundering and ultimately take away the proceeds of crime from criminals.

5.1 Understanding risk

Malawi undertook a review of its National Risk Assessment between November 2017 and June 2018. The report has highlighted areas that are prone to generating proceeds that are subsequently laundered in the financial system. The report further recommends that stakeholders should conduct sectoral or self-risk assessments in view of the highlighted typologies. This will ensure that stakeholders understand risks and are able to employ effective mitigating measures. For example, relevant government departments and reporting institutions can focus its mitigating measures on their vulnerable areas.

5.2 Use of FIA's intelligence capabilities

LEAs are encouraged to make use of the FIA to obtain information on cases that fall under their purview. FIA has powers to postpone transactions (freeze accounts) and apply other provisional measures that can be useful to LEAs. The FIA's financial analysis is an effective approach to complement investigations into predicate crimes, i.e. LEAs can make use of the FIA to conduct parallel financial investigations.

5.3 Enhanced access to beneficial ownership information by authorities and stakeholders

The use of fake or false business certificates to open accounts has revealed loopholes that are being exploited by criminals. It is therefore imperative that stakeholders such as reporting entities and authorities including the FIA should have direct access to information about the beneficial owner of companies in order to avoid the financial system being used by criminals. Registered companies are expected to file returns such as financial statements to the Registrar of Companies. This information, coupled with the use of the Credit Reference Bureau, can mitigate losses incurred through loan kiting, among other crimes.

5.4 Use of the media

Financial institutions stand to benefit from the use of publicly available information, particularly from the media, to screen out undesirable elements on their books. More often than not, media outlets have been instrumental in publicising financial crime when authorities have made arrests or there are ongoing cases in the courts. This information can prove useful in profiling persons of interest as well as gathering information for Suspicious Transaction Reporting.