



**MONEY LAUNDERING
TYPOLOGY STUDIES REPORT
DEVELOPED BY THE FINANCIAL
INTELLIGENCE CENTRE, GHANA
FOR
ACCOUNTABLE INSTITUTIONS**

JULY, 2019



**MONEY LAUNDERING
TYPOLOGY STUDIES REPORT
DEVELOPED BY THE FINANCIAL
INTELLIGENCE CENTRE, GHANA
FOR
ACCOUNTABLE INSTITUTIONS**

JULY, 2019

TABLE OF CONTENTS

| | |
|---|----|
| LIST OF ACRONYMS | iv |
| 1.0 Executive Summary | 1 |
| 2.0 Introduction | 2 |
| 3.0 Background | 3 |
| 4.0 Overview of STRs Received | 3 |
| 4.1 General Observations on the STRs Received | 4 |
| 5.0 Money Laundering Techniques | 4 |
| 5.1 Money Laundering Typologies | 5 |
| 5.1.1 Typology 1: Fraud | 5 |
| Inheritance Fraud | 5 |
| Visa Processing Fraud | 6 |
| Fraud Associated with the Football Profession | 7 |
| Misrepresentation/false pretenses | 7 |
| Investment Fraud | 8 |
| Hacking into accounts | 9 |
| Procurement fraud | 9 |
| Bank employee fraud | 10 |
| Collusion between bank employee and customer fraud | 10 |
| Cloned Cheque | 11 |
| Gold scam | 13 |
| ATM Card Fraud | 12 |
| 5.1.2 Typology 2: Trade Based Money Laundering | 12 |
| Supply of Shea Butter | 13 |
| Over invoicing of goods | 13 |
| Funds received for the purchase of high value goods | 14 |
| 5.1.3 Typology: 3: Drug trafficking | 14 |
| Legitimate business used as front | 14 |
| Association with drug traffickers | 15 |
| 5.1.4 Typology 4: Tax evasion | 16 |
| Association with a Politically Exposed Person (PEP) | 16 |

| | |
|---|----|
| Advance payment of taxes on new entities | 16 |
| Sham movement of goods as a bait to evade tax | 17 |
| 5.1.5 Typology 5: Counterfeiting of Currency | 17 |
| Fake Currency deposited into the financial system | 17 |
| New bank account receiving fake currency | 18 |
| Bank customer deposit fake currency | 18 |
| 5.1.6 Typology 6: Use of foreign bank accounts | 19 |
| Transfer of funds through foreign bank account | 19 |
| 5.1.7 Typology 7: Insurance Fraud | 20 |
| False Death Claim | 20 |
| False Hospitalization Claim | 20 |
| False fire Insurance Claim | 20 |
| 5.1.8 Typology 8: Securities fraud | 22 |
| Investment fraud | 22 |
| Frequency of funds used for investment | 22 |
| 6.0 Conclusion | 23 |
| 6.0 Recommendations | 23 |

ACRONYMS

| | | |
|---------|---|---|
| AML/CFT | — | Anti-Money Laundering/Countering the Financing of Terrorism |
| ATM | — | Automatic Teller Machine |
| CDD | — | Customer Due Diligence |
| FATF | — | Financial Action Task Force |
| FIC | — | Financial Intelligence Centre |
| FIU | — | Financial Intelligence Unit |
| GIABA | — | Inter-Governmental Action Group against Money Laundering in West Africa |
| ID | — | Identity |
| LC | — | Letters of Credit |
| MOU | — | Memorandum of Understanding |
| PEP | — | Politically Exposed Person |
| STR | — | Suspicious Transaction Report |
| LEA | — | Law Enforcement Agency |
| ML/TF | — | Money Laundering/ Terrorist Financing |

1.0 Executive Summary

This is the FIC's first money laundering typology report. The report contains trends and patterns observed from Suspicious Transaction Reports received from financial institutions (banking, insurance and the securities sectors) as well as feedback from competent authorities on investigations on money laundering cases from 2014 -2018.

This typology study covers a number of predicate offences of money laundering including fraud, trade-based money laundering, drug trafficking, tax evasion, counterfeiting of currencies, use of foreign bank accounts, false insurance claims and investments schemes. The study considers the predicate offences as the grounds on which the proceeds of crime are derived. Each predicate offence is studied for several schemes and real cases were used for this exercise. For instance, fraud as a predicate offence had twelve (12) different schemes such as inheritance fraud, visa fraud, football profession fraud, misrepresentation, investment fraud, hacking into accounts, procurement fraud, bank employee fraud, collusion between bank official and customer, cloned cheques, gold scam and ATM card fraud. The other types of predicate offences have also been discussed in detail in the report.

The FIC has been instrumental in assisting Law Enforcement Agencies (LEAs) particularly in the area of providing financial intelligence to both domestic and international counterparts through Memorandum of Understanding (MOU) and other international instruments.

The fight against money laundering can only be achieved through enhanced inter-agency collaboration of relevant stakeholders and LEAs. Competent authorities and stakeholders in the fight against ML/TF have come together to handle a significant number of predicate offenses and chalked a number of successes in the investigation, prosecution and conviction of money laundering cases.

The FIC has also included trends observed in the reporting of STRs in the period under review. There were a number of techniques used by the perpetrators of money laundering. These include the use of third parties, providing false information to meet customer identification requirements, use of professionals (lawyers, accountants, tax consultants, notaries etc.), use of ATM cards, use of fake ID cards and emerging new technologies among others.

2.0 Introduction

The Financial Action Task Force (FATF) is the global body mandated to set standards on Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT). The FATF has set Forty (40) Recommendations for countries to implement in order to ensure that the international financial system is not abused by criminals.

Recommendation 29 of the Financial Action Task Force (FATF) 40 Recommendations enjoins countries to establish a Financial Intelligence Unit (FIU) that serves as a national Centre for the receipt and analysis of: (a) Suspicious Transaction Reports (STRs); and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis. It further states that the FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that is required to undertake its functions properly.

Additionally, the Interpretative Note to the recommendation stipulates that, FIUs should add value to the information received from reporting entities and also conduct strategic analysis to identify Money Laundering and Terrorist Financing (ML/TF) related trends and patterns. This information can be used by the FIU or other state entities in order to determine ML/TF related threats and vulnerabilities. The outcome of this analysis may also help to establish policies and goals for the FIU, or more broadly for other entities within the AML/CFT regime.

In view of the above, the Financial Intelligence Centre (FIC) was established by Section 4 of the Anti-Money Laundering Act, 2008 (Act 749), as amended, as the national Centre for the receipt, analysis and dissemination of financial intelligence. The objects of the Centre as prescribed by section 5 of the Act are as follows:

- a. assist in the identification of proceeds of unlawful activity;
- b. assist in the combat of
 - i. money laundering activities
 - ii. financing of terrorism
 - iii. financing of the proliferation of weapons of mass destruction
 - iv. any other transnational organized crime
- c. make information available to investigating authorities, the intelligence agencies and the revenue agencies to facilitate the administration and enforcement of the laws of the Republic; and
- d. exchange information with similar bodies in other countries as regards money laundering activities and similar offences.

The FIC aims to protect the Ghanaian economy from the scourge of money laundering and terrorist financing. In this regard, the FIC undertakes typology studies to better understand prevalent schemes on money laundering in Ghana and to enable stakeholders to appreciate global efforts on AML/CFT standards. The results of the study also provide decision makers with a scope within which policies on money laundering threats could be developed.

3.0 Background

The outcome of Ghana's First Round of Mutual Evaluation exercise conducted by the Inter-Governmental Action Group against Money Laundering in West Africa (GIABA) in November 2009 revealed that, the FIC, the National Centre for the receipt of STRs was not operational. The assessment further revealed the following:

- no guidance to direct reporting entities to submit STRs to the FIC.
- lack of awareness of the obligation to submit STRs across all reporting entities.
- lack of statistics on money laundering across all sectors.

Although Ghana has put in efforts to address the above deficiencies, a comprehensive trend and patterns of money laundering schemes is yet to be developed.

Again, in September 2016, Ghana was subjected to the Second Round of Mutual Evaluation process conducted by the Inter-Governmental Action Group against Money Laundering in West Africa (GIABA). GIABA is a specialized institution set up by the Economic Community of West African States (ECOWAS) to oversee the implementation of AML/CFT measures within the sub-region. GIABA conducts mutual evaluations of ECOWAS member States to assess the level of compliance and also to recommend ways to improve the AML/CFT regime. During the conduct of the Second Round of Mutual Evaluation of Ghana, the assessment team observed that, Ghana needed to develop typology study on money laundering schemes, patterns and trends for reporting entities to assist in the filing of STRs to the FIC.

The team also recommended that Ghana produced a typology study on money laundering to serve as a guide to Accountable Institutions so as to increase the filing of STRs to the FIC.

In view of this, the FIC is poised to provide continuous training and guidance to Accountable Institutions and also to encourage them to monitor and report on red flags associated with money laundering schemes. The FIC has put this typology study together based on Suspicious Transaction Reports received from Accountable Institutions and feedback from the Law Enforcement Agencies (LEAs) as well as other international counterparts on trends, patterns and techniques observed from 2014 -2018.

4.0 Overview of STRs Received

Below is a general overview of STRs received from accountable institutions, analysed and/or disseminated to relevant LEAs. This overview is to provide feedback to the accountable institutions and to help them enhance their AML/CFT compliance regime and particularly to identify and file STRs to the FIC.

This typology report covers STRs that were received and analysed from the various financial institutions (banking, insurance and the securities sectors) between 2014 and 2018. Most of the reports were received from banks, analysed into actionable intelligence and disseminated to both domestic and international law enforcement agencies.

4.1 General Observations on the STRs Received

- Personal bank accounts being credited regularly with relatively huge sums of funds without any known business and source of income.
- Customer's unwillingness to provide further information when requested by a financial institution and subsequently terminating the business relationship.
- Customer providing falsified financial account to obtain a loan, credit or overdraft facility from a financial institution.
- Multiple unrelated remitters sending funds to the same beneficiary without any known business relationships.
- Dual/multiple identities of customers.
- Unwillingness of customers to update KYC/CDD information with financial institutions.
- Use of third party accounts to receive funds.
- Account activity inconsistent with a customer's known profile.
- Lack of disclosure of sources of income by customers of financial institutions.
- Forged and false documents presented to financial institutions.
- Large sums of cash deposits from multiple sources into a newly opened account.
- Under-declaration on KYC forms of expected turnover and source of income during account opening process.
- Fraudulent insurance claims.
- Fraudulent investment schemes.

5.0 Money Laundering Techniques

This typology report was conducted on Suspicious Transaction Reports (STRs) received, analysed, disseminated and feedback from Law Enforcement Agencies (LEAs) between 2014 and 2018. The FIC observed emerging trends of money laundering and its associated techniques used in the review period. These techniques include the following:

- Use of wire transfers and remittance services providers to receive fraudulently obtained funds.

- Use of third parties to receive and transfer illicit proceeds.
- Use of currency exchanges within the financial system.
- Providing false information to meet customer identification requirements.
- Use “gatekeepers” professional services such as lawyers, accountants and notaries to obscure the identity of beneficiaries and the source of illicit funds.
- The use of emerging payment technologies including the use of ATM cards.
- Use of the internet (misrepresentation and hacking into accounts).
- Use of high value assets such as the development and sale of real estates and the sale of gold.
- Use of trade mis-invoicing.
- Use of schemes to evade the payments of appropriate taxes.
- Use of employees within the financial system to avoid detection.

5.1 Money Laundering Typologies

5.1.1 Typology 1: Fraud

Fraud can be described as the wrongful or criminal deception intended to result in financial or personal gain. This typology is usually perpetrated by a person or an entity and it is intended to deceive others, typically by unjustifiable means.

Inheritance Fraud

Case Study 1.1

- C (female) established an amorous relationship with B (male) via the internet (facebook). In the course of their online dating, C purportedly misrepresented herself to B as a USA citizen and orchestrated her gold scam scheme using inheritance as a bait.
- C managed to convince B about an estate that was bequeathed to her by her late father who owned a mining business in Ghana.
- C subsequently introduced B to her attorney, D, after he had agreed to assist her navigate the probate process.
- B and D exchanged series of emails on the purported processes involved in acquiring the estate and the gold. D managed to convince B to make a first transfer in November, 2018, being fees associated with the storage of gold in Ghana. The funds were transferred into a bank account of a company established by D. Upon receipt of the funds into the company’s account, D issued further instructions to the bank to transfer the funds into his personal account.
- During due diligence by the bank, D was unable to present relevant documentations requested to complete the process thereby arousing the suspicion of the bank.
- D was apprehended by the Police and currently the matter is under investigations.

Indicators/ Red flags

- Use of wire transfers.
- Use of third parties to receive and transfer illicit proceeds.
- The provision of inconsistent information during due diligence.
- Transfer of funds received on company account into personal account.
- The use of technology and social media in identifying and targeting potential victims.
- Use “gatekeepers” professional service providers (lawyers, accountants, brokers etc) to obscure identity of beneficiaries and the source of illicit funds.

Visa Application Fraud

Case Study 1. 2

- On August 4, 2015, Bank A received a bank statement of customer B from an Embassy to confirm if the bank statement was authentic. The bank statement was used as part of documentation to apply for visa for applicant C, also a customer of Bank A. The Embassy suspected that the applicant, C, had forged the bank statement of customer B and so contacted the bank for verification.
- The Embassy was verifying the bank statement from Bank A as part of its due diligence conducted on visa applications.
- During the conduct of internal investigation, Bank A noted that there were differences between the biodata (photo, date of birth) of the passport information and the details on the ID card presented by Customer C during the account opening process. Bank A further noted that most of the transactions on Customer C’s account were conducted through ATM cards by third parties.
- Bank A also noted that a letter purportedly signed by customer B was received on September 3, 2015 requesting the bank to change the phone number provided during the account opening process as he was located in a different region in the country. The bank therefore asked the purported customer to report at the branch where customer B claimed to be residing in order to complete due diligence procedures and verification processes.
- Bank A further observed that customer B and Visa applicant C had provided same addresses and place of work at the time of account opening.
- Analysis of the account information by the FIC revealed that same third parties transacted on both accounts and both had presented fake ID cards to open accounts.
- The case was referred to the Visa Fraud section of the Criminal Investigation Department of Ghana Police Service.

Indicators/ Red flags

- The use of same third parties to make deposits and withdrawals on both customers’ accounts.
- The use of ATM cards to conduct most of the transactions.

- The presentation of fake ID cards.
- Use of fake bank statements.

Fraud Associated with the Football Profession

Case Study 1.3

- The FIC received a report from Bank Q on subject purporting to be a footballer and using his account to receive several inflows from different unrelated persons.
- In July 2015, Customer D opened an account with Bank Q and gave his profession as a footballer with a foreign football club and the purpose of the account was to receive remittances from his manager (residing outside the country).
- During a routine bank monitoring process, Bank Q noted that, Customer D had received several inflows from different remitters from different jurisdictions.
- In March 2017, Customer D's account received two remittances of US\$33,980.00 and US\$64,990.00 from unconnected remitters.
- During due diligence, customer D claimed that, one of the remitters was his football agent but could not present relevant documentation to support his claim.
- Bank Q was not convinced about his explanation surrounding the source and purpose of the funds and thereby escalating the matter to the FIC.
- The FIC directed Bank Q to return the funds to the remitters and notified the various Embassies of the remitters to inform them of the suspected fraud by customer D.
- The matter was referred to a Law Enforcement Agency for investigations.

Indicators/ Red flags

- Opening of Foreign Currency and Exchange account purposely to receive remittances.
- Use of wire transfers as well as the volume and frequency of inflows.
- Use of different unconnected remitters from different jurisdictions.
- Inability to present relevant documentation.
- Use of high earned profession such as footballer to avoid suspicion and monitoring of the Bank.

Misrepresentation/False Pretenses

Case Study 1.4

- During a periodic account monitoring by Bank G, it was revealed that Customer F was reported in the media for defrauding a Swiss couple of an amount of US\$68M and US\$170,000.00 by false pretenses.

- The publication further revealed that, Customer F was among a syndicate perpetrating fraud in the capital, Accra.
- In February, 2018, the FIC was informed of an inflow of US\$116,145.00 received on Customer F's account with another Bank H. Customer F could not convince Bank H on the source and purpose of the funds thereby arousing the suspicion of Bank H.
- The case was referred to a Law Enforcement Agency for investigations.

Indicators/ Red flags

- Adverse media publications on customers and associates.
- Use of wire transfers as well as the volume and frequency of inflows on the account.
- Use of different unconnected remitters from different jurisdictions.
- Inability to establish the source and use of the funds.
- Association with alleged criminal syndicate.

Investment Fraud

Case Study 1.5

- The FIC received an STR of which company T's account received an inflow of US\$191,922.00 at Bank P.
- Company T indicated its nature of business as dealers in vehicles at the account opening stage. Meanwhile, company T claimed the funds were to be invested in real estates so some of the funds were to be used for the rental of cranes to clear the land for development.
- While conducting due diligence, Company T provided land documents in a different name to the bank thereby arousing the suspicion of the Bank. Company T could not also provide Bank P with any contractual agreement with the remitter.
- Further intelligence received by the FIC indicates that the remitter sent the funds to company T for the storage of gold bars and not real estate development. It was also revealed that the remitter met with a representative of Company T via social media (facebook). Company T informed the remitter to indicate 'real estate development' on the SWIFT information covering the remittance although there was no intention for real estate development.
- The case was referred to a Law Enforcement Agency for investigations.

Indicators/ Red flags

- Inconsistencies in the ownership of title documents of land.
- Use of wire transfers as well as the volume and frequency of inflow on the account.
- Lack of relevant documentation to back purported contract.
- Use of the internet.
- Inconsistencies in the purpose of remittances.

Hacking into accounts

Case Study 1.6

- The FIC received an STR in which a customer of Bank S was alleged to be involved in hacking into the bank accounts of unsuspecting victims.
- On April 20, 2018, customer G's account received an inflow of US\$16,000.00 in two tranches (US\$9000.00 and US\$7,000.00).
- Again, on April 23, 2018, Bank S received an inflow of US\$8,900.00 in favour of customer G from a different remitter.
- On April 27, 2018, Bank S received an email correspondence from an alleged foreign victim about customer G hacking into his account and diverting funds into his account with Bank S.
- The FIC directed Bank S to return the funds to the remitter on grounds of fraud.
- The case was referred to the Law Enforcement Agency for investigations.

Indicators/ Red flags

- Email correspondence from an unsuspecting victim.
- Use of wire transfers as well as the volume and frequency of inflow on the account.
- Use of the internet to hack into bank accounts.

Procurement fraud

Case Study 1.7

Procurement fraud can be defined as dishonestly obtaining an advantage or causing a loss or employing other unfair means during procurement process by public servants, contractors or any other persons involved in the procurement.

- On May 8, 2018, Company A won a sole sourced contract to supply 75,000 litres of insecticides at a rate of US\$103.5 per litre amounting to a total of US\$7,762,500.00 through the Public Procurement Authority.
- On May 20, 2018, Bank A issued a Letter of Credit supposedly for the shipment of 76,640 litres at the rate of US\$69.68 per litre totaling US\$5,340,000.00 to Company B with a supporting invoice from Company A.
- During investigation, it was revealed that the contract was originally priced at US\$4,032,000.00 with the manufacturer of the product and therefore a profit of US\$3,730,500.00 was made by Company A.
- The case was referred to the Law Enforcement Agency for investigations.

Indicators/ Red flags

- Unfavorable open source information on customer.
- Use of Letters of Credit (LC) for the shipment of goods.
- Procurement process not clear.
- Possible relationships existing on sole sourced contracts.

Bank Employee Fraud

Case Study 1.8

- On December 2018, customer U filed a complaint to Bank F that the balance on her account was supposed to be GH¢33,000.00 and not GH¢2,000.00 as indicated on her bank statement.
- Bank F initiated an internal investigations into the account and noted that cash withdrawal of GH¢31,000.00 was conducted over the counter on November 16, 2018.
- When Customer U was queried by Bank F, she indicated that she did not know about any withdrawal made on the said date over the counter.
- Further investigations by Bank F revealed that, a bank official had forged the signature of Customer U and withdrawn an amount of GH¢32,000.00 from her account without authorization.
- Bank official was immediately arrested by the Police and processed before court. Bank F has further terminated the appointment of the bank official.

Indicators/ Red flags

- Change in employees' life style.
- Forged signature of customer
- Cash withdrawn without relevant documentation including photo copies of ID cards.

Collusion between bank employee and customer fraud

Case Study 1.9

- Customer R received an amount of GH¢110,610,000.00 on his account domiciled with Bank A. The funds credited into the account were alleged to have been transferred by Customer R himself and not Bank A.
- On July 3, 2017, Customer R unlawfully accessed the bank's payment system through a local IP address of the bank. Customer R further logged into Bank A's payment system using the credentials of a staff of Bank A and transferred the said amount into his account.
- On July 4, 2019, Customer R transferred an amount of GH¢170,000.00 into the accounts of his accomplices domiciled with three different banks.
- A total amount of GH¢84,991.06 was withdrawn by Customer R and his accomplices by ATM cards from other jurisdictions.

Indicators/ Red flags

- Use of bank staff credentials to log into payment system.
- Collusion between customer and bank official to facilitate illegal transactions.
- Use of the internet/ IP addresses of the bank.
- Use of ATM cards.

- Accessing funds from different jurisdictions.
- Transfer of funds without any verifiable economic purposes.

Cloned Cheque

Case Study 1.10

- Company R issued a cheque of GH¢ 350,000.00 to be drawn on a closed account domiciled with Bank L for the benefit of customer G of another Bank P.
- The cheque was meant for the payment of 100 motor bikes.
- The cheque was cleared and credited to the account of customer G.
- Bank L noted that the transaction was fraudulent and requested Bank P to return the GH¢ 350,000.00.
- During investigation by Bank P, it was revealed that customer G's account had received a number of cheque deposits.
- Between December 29, 2015 and January 7, 2016, a cheque with face value of GH¢ 11,100.00 was presented on four different occasions but was not paid.
- The matter was reported to the Law Enforcement Agency for investigations.

Indicators/Red flags

- Cheques dishonored on several occasions.
- Use of closed account for cheque deposit.
- Receipt of several cheques on account without any verifiable economic reasons.

Gold Scam

Case Study 1.11

- The FIC received an STR in which a syndicate of fraudsters masterminded by a Ghanaian who lures foreigners into fake gold businesses in Ghana.
- In their proposal, interested investors must visit Ghana and open a “metal account” where all funds for the transaction would be deposited.
- In the instant case, the foreigners/buyers signed an agreement for the purchase of 200kg of gold each. They were then taken to a bank where a safe deposit box containing some metals, alleged to be gold, were shown to them to gain trust.
- As part of the modus operandi, a sample of the gold (2kg) was sent to a refinery in Country M to be tested and confirmed for shipment. The 2kg gold was confirmed to be pure and subsequently delivered to the buyers in anticipation that the remaining 198kg would be tested and delivered at a later date to be agreed upon.
- The investors were lured to pay over US\$250,000.00 each to cover several costs including storage, invoice, shipping and delivery.

- The purported 198kg of gold was never delivered.
- The matter was referred to the Ghana Police for investigation.

Indicators/Red flags

- Use of wire transfer and the volume of funds.
- Use of bank services (safe deposit box)
- Use of gold as an attractive item.
- Use of business agreement between natives and foreigners.
- Use of prepayment schemes such as payment including storage, invoicing, shipping and delivery.

ATM Card Fraud

Case Study 1.12

- The FIC received an STR in which nine (9) individuals opened separate bank accounts at the same branch of a Bank J within the same period. The nine (9) individuals provided similar addresses and contact details during the account opening process.
- All the nine accounts were funded with huge cash deposits from the account holders and unknown third parties.
- Within two months, the average total cash deposits in each of the accounts was GH¢200,000.00.
- Funds credited into the accounts of these persons were immediately withdrawn by a third party in China through ATM transactions.
- Intelligence received by the FIC revealed that the third party residing in China conducted an average of forty-eight (48) ATM withdrawals totaling GH¢60,000.00 on daily basis.
- The matter was referred to the Bank of Ghana for investigations.

Indicator/ Red flags

- Individuals using same details to open bank account at the same branch.
- Unusual or several ATM withdraws from other jurisdictions.

5.1.2 Typology 2: Trade Based Money Laundering (TBML)

Trade-based money laundering remains a major threat globally. There is an emerging trend whereby importers and some personnel of financial institutions collude to avoid the conduct of proper due diligence and engage in over and under invoicing schemes. This type of money laundering usually involves invoice manipulation and uses trade finance routes and commodities to avoid financial transparency and the payments of tax obligations.

Supply of Shea Butter

Case Study 2.1

- The FIC received an STR in which between November 17, 2017 and January 26, 2018, Customer B received eight (8) inflows totaling US\$22,000 from four (4) different remitters for the supply of shea butter and personal payments.
- On May 8, 2018, Customer B's account further received two remittances of US\$11,812.06 from two separate remitters from the United States of America. Customer B claimed the inflow was to pre-finance the supply of shea butter.
- During due diligence, Customer B only provided invoices and sales agreement purportedly covering the export of the shea butter but was unable to present relevant documentations covering the exportation of the shea butter.
- Also, documents presented were confirmed as forged by the bank. Customer B further presented a letter to the bank instructing them to return the funds.

Indicators/ Red flags

- Use of wire transfers as well as the volume and frequency of inflows on the account.
- Different unconnected remitters from different jurisdictions.
- Inability to present relevant documentation to support claims.
- Customer instructing bank to return the funds to the remitter.

Over Invoicing of Goods

Case Study 2.2

- During a routine monitoring of accounts by Bank R, it was revealed that Customer E's account had received a number of cash deposits and several trade related cheque deposits from other business clients.
- Customer E opened account with Bank R in June 2011 and indicated Aluminum and Metal fabrication as his profession.
- In March 2016, Bank R initiated investigations into the activities of Customer E and it was observed that Customer E had presented invoices that were higher than the values indicated by Customs. Bank R therefore rejected the payment on grounds of over-invoicing.
- The matter was referred to LEA for investigation.

Indicators/ Red flags

- Presentation of over invoiced documents.
- Several trade related cheque deposits made into an account without any verifiable economic reasons.
- Inconsistencies between the invoice values and customs declared values.

Funds received for the purchase of high value goods

Case Study 2.3

- Bank M received a remittance of EUR40,000.00 in favour of Company H from an unconnected remitter. Company H indicated during account opening that the account was to be funded with business proceeds and made an initial deposit of GH¢100.00.
- During due diligence by Bank M, Company H claimed that the remitter was a business partner and funds were meant to purchase logistics and equipment for event organising.
- Company H further provided a bill of lading listing four (4) cars and other personal effects to be cleared at the port as documentary evidence supporting the purpose of the funds in question. Bank M was not convinced with the explanation and thereby filed an STR to the FIC.
- Intelligence received by the FIC indicated that though the remitter had been a victim of gold scam, he was also being investigated for fraud and embezzlement in his country of residence.
- The FIC directed the freezing of the transaction and referred the matter to law enforcement agency for investigations.

Indicators/ Red flags

- Inability to provide business agreement to support his claim.
- Inconsistencies in the purpose of the remittance.
- Involvement in the circle of crimes by unsuspecting victims.

5.1.3 Typology: 3: Drug Trafficking

Criminals manufacture, distribute and sell psychotropic substances for financial benefits. When such criminals are busted for trafficking in drugs, competent authorities should be made to identify and trace all assets linked to the proceeds of the crime. In Ghana, this type of crime is usually operated by a syndicate and therefore investigations are likely to rope in a number of cartels.

Legitimate Business Used as Front

Case Study 3. 1

- Intelligence received by the FIC indicated that Company A was about to receive an amount of US\$170,000.00 from a jurisdiction known for the transportation and trading in narcotics.
- In April 2013, the director of Company A was involved in a currency seizure of US\$650,000 at the Kotoka International Airport, Accra. Preliminary investigations revealed that the currency was intended to pay for the shipment of cocaine from South America.

- Further investigations revealed that a senior manager of Company A had earlier been charged and convicted in 2002 for fraud and money laundering in Dubai and served a 10 year term in jail.
- Further intelligence indicated that the director of Company A also defrauded victim B, a Senegalese of an amount of EUR150,000.00.
- Victim B lodged a complaint with the Ghana Police Service in September 2016 and the director of Company A was arrested in October 2016.
- Again, in September 2018, Company A attempted to defraud another victim at the Kotoka International Airport, Accra but for the timely intervention of a Law Enforcement Officer who profiled and disrupted the operations of Company A. The director of company A and his associates were arrested.
- In the course of investigations, the Law Enforcement Agency recovered fake gold and other equipment used to defraud victims by Company A and its cohorts. Investigation is ongoing.

Indicators/ Red flags

- Use of wire transfers as well as the high volume inflows on the account.
- Subject and associates linked with previous criminal activities.
- Evidence of defrauding of unsuspecting victims.
- Association with jurisdictions known for drug trade.
- Involvement in previous case of cash smuggling.

Association with Drug Traffickers

Case Study 3. 2

- The FIC received intelligence on Company J for its involvement in drug trafficking and money laundering activities.
- The FIC further requested for financial information from Bank L to review transactions on the account. Bank L noted that Company J's account had received an amount of GH¢35,000,000.00 from a customer of another Bank P.
- In order to avoid detection, Company J quickly issued four (4) cheques to four (4) customers of four different banks. One of the four banks returned the funds to Bank L due to unsatisfactory due diligence on the purpose of the funds.
- Bank L further observed that Company J is associated with two (2) drug traffickers who have been convicted in the United Kingdom.
- The case was referred to LEA for investigations into the activities of Company J.

Indicators/ Red flags

- Use of wire transfers as well as the volume of inflows on the account.
- Customer associated with convicted criminals.

5.1.4 Typology 4: Tax evasion

Corporate entities and individuals can employ schemes that would enable them to evade the payment of appropriate taxes on their taxable income. Financial Institutions are to monitor transactions on customers account and escalate the issue of possible tax evasion to the FIC for further action.

Association with a Politically Exposed Person (PEP)

Case Study: 4.1

- Bank F received a deposit of US\$1million on behalf of Mr. B, a customer of the bank from a law firm. Bank F noted that, the amount deposited was inconsistent with the mandate and known transactions on Mr. B's account.
- As part of due diligence by Bank F, Mr. B failed to provide satisfactory explanation and relevant documentation to establish the source and purpose of the funds in question.
- Further investigations revealed that, the funds were proceeds from the sale of a property in a prime area in Accra. Mr. B was found to be related to a PEP.
- The matter was referred to LEA for further investigations.

Indicators/ red flags

- Use of professional service providers of a 'Gate Keeper' (a law firm).
- Inconsistency in known transactions on the account.
- Insufficient explanation by account holder and absence of relevant documentation.
- Association with a Politically Exposed Person (PEP).

Advance Payment of Taxes on New Entities

Case Study 4.2

- In February 2014, Bank A filed an STR in which Company XYZ received a remittance of US\$43,569.45.
- As part of due diligence, Company XYZ indicated that the funds were for the payment of upfront taxes for a new Company UVW which was yet to be established.
- Bank A further noted that Company XYZ's account was solely funded by foreign remittances from unrelated persons and entities.
- Intelligence received by the FIC indicated that Company XYZ attempted to defraud some foreigners to the tune of US\$450million.
- The FIC directed the freezing of account of Company XYZ and referred the matter to Law Enforcement Agency for investigations.

Indicators/ red flags

- Insufficient documentary evidence to establish the purpose of funds.
- Several remittances from unconnected persons without any justifiable purposes.

Sham Movement of Goods as a Bait to Evade Tax

Case Study 4.3

- Bank A provided Company PQR with a Buyers Credit Facility (Traders Loan) of US\$1,082,932.59 to expedite its business activities with clients abroad.
- On January 2015, company PQR made another request to Bank A to effect payment of US\$300,000.00 on its behalf to its suppliers from Country G.
- A review of documents by Bank A indicated that Company PQR, provided; pro-forma invoice instead of final invoice for the payment request; an invalid custom declaration number with incorrect dates and duty details; a wrong vessel details which did not correspond with the physical location and existence details of the vessel and the container number on the document was inconsistent with international standards.
- At the end of the internal investigation by Bank A, it was concluded that there were no physical movement of goods and that Company PQR had forged all the documents in order to facilitate the release of credit facility to his counterparties abroad.
- Meanwhile, Company PQR's account had received several remittances amounting to US\$298,288.34 and transfers from various organisations amounting to GH¢1,214,658.11.
- A comprehensive Tax Audit was conducted and the company was served with a notice to pay taxes of GH¢2,471,951.04 due to the state.
- The case is being investigated by a competent authority.

Indicators/ Red flags

- Use of wire transfer and the volume of funds involved in the transactions.
- Use of forged documents
- Involvement with foreign businesses on credit facility and other forms of inconspicuous arrangements.

5.1.5 Typology 5: Counterfeiting of Currency

Fake Currency Deposited into the Financial System

Case Study: 5.1

- Bank M received a call from Company B, a customer of the bank that a third (3rd) party would be making a deposit of EUR200,000, all in EUR 500 denominations into Company B's account and wanted to find out if the denomination was in use.
- The directors of Company B were former employees of Bank M.
- The cash amount of EUR200,000.00 was received by Bank M from the third party. The bank teller who received the cash observed that most of the EUR500 bills were rejected by the money counting machine. Out of the EUR200,000.00 only EUR18,500.00 was accepted as genuine bank notes by

Bank M and the remaining amount returned to Company B as fake.

- On August 2, 2016, another customer W of Bank M instructed the bank to debit his account in exchange of EUR5,000.00. Customer W travelled to France and after spending EUR500 out of the EUR5,000.00 given to him by Bank M, the remaining EUR4,500.00 were declared as fake by another Bank Q in France.
- Customer W returned the remaining funds to Bank M in Ghana. The bank initiated investigations into the matter and run the bills through its Currency Detection Machine and the bills were accepted as genuine bank notes.
- Again, Bank M subjected the notes to a second check through the assistance of the regulator and found out that the EUR500 notes were all fake currencies.
- Bank M contacted Company B about the outcome of the internal investigation conducted on the veracity of the notes.
- The matter was reported to the Law Enforcement Agency for investigations.

Indicators/ Red flags

- Unknown source of funds.
- Use of third parties.
- Unusual enquiry by customer prior to deposit.
- Involvement of ex-employees of the bank.

New Bank Account Receiving Fake Currency

Case Study: 5.2

- The FIC received an STR in which two persons operating a joint account at Bank H opened a EUR account on September 16, 2016.
- The two made an initial deposit of EUR4,000.00 into the account.
- During the counting of the cash, Bank H detected that the EUR notes were fake.
- The case was referred to Law Enforcement Agency for investigations.

Indicators/ Red flags

- Unknown source of funds.
- Fake currencies presented for deposit into the account.
- Use of a new account for voluminous transactions.

Bank Customer Deposits Fake Currency

Case Study: 5.3

- The FIC received an STR in which a foreign national P, a customer of Bank V deposited an amount of GH¢3,250.00 in GH¢10.00 notes.
- Bank V teller detected that all the said amount was fake.
- When Bank V inquired from the foreign national P, he claimed that the cash

was received from his business clients as payments of goods supplied.

- The matter was referred to law Enforcement Agency for investigations.

Indicators/ Red flags

- Lack of evidence to support source of funds.
- Fake currencies presented for deposit into the account.

5.1.6 Typology 6: Use of Foreign Bank Accounts

The use of foreign bank accounts remains an attractive channel for criminals to hide and transfer proceeds of crime to associates in other jurisdictions. Financial Institutions are therefore to ensure that high risk customers such as dealers in high value goods, domestic and foreign PEPs are subjected to enhanced due diligence regarding the source of funds deposited into financial institutions.

Transfer of Funds through Foreign Bank Account

Case Study 6.1

- In November 2011, Ms. C a staff of Bank BVB was approached by Madam PQ for the transfer of US\$1,180,000.00. Ms. C did the necessary verifications and forwarded the request to the payment center of Bank BVB.
- As part of due diligence, Madam PQ presented her husband's passport and marriage certificate in support of the transaction. Madam PQ began to call the bank when the transfer was delayed and Ms. C referred her to the branch manager since the matter was above her.
- Ms. E, the Compliance Manager of Bank BVB, referred the matter to the regulator represented by Mr. A. Upon review of the documents, Mr. A identified some irregularities; the property in question was located at Trasacco Valley and was purchased 3months prior to the sale, cost of the house was higher than the sale proceeds of US\$1,180,00.00 received by the bank. The regulator advised Bank BVB to obtain evidence showing that the funds were transferred to the country and not generated internally.
- Due to these irregularities, Mr. A advised the Central Bank to decline the request by Bank BVB and direct the bank to confirm whether they have complied with the AML provisions.
- Mr. A called one Ms. M (who signed the letter requesting the transfer approval) to enquire whether she was aware of the details surrounding the property. Ms. M claimed to have no knowledge of the property details.
- Ms. M's lawyer subsequently threatened legal actions due to the delay in the transaction.
- Bank BVB transferred the funds as instructed despite the intervention of the regulator.
- The matter was subsequently reported to the FIC.
- Staff and management of BVB Bank were arrested and prosecuted.

Indicators/ red flags

- Use of wire transfer as well as the volume of funds involved.
- Use of the sale of property to disguise the source of funds.

Deposit of Foreign Currencies into New Foreign Bank Account

Case Study 6.2

- Bank A filed an STR on Company ABC whose directors are Mr. A, a national of Country N and Mrs. Q, a Ghanaian.
- In April 2014, Mr. A conveyed US\$2,493,300.00 to XYZ Bank in Ghana for the purpose of opening an account with the bank. However, owing to the unsatisfactory due diligence, the Bank refused to open the account.
- The said amount of US\$2,493,300.00 was later conveyed from Bank XYZ in a bullion van of another Bank FTX in the company of the Ghanaian director Mrs. Q.
- Bank FTX transferred US\$1,709,330.41 from the said amount to various jurisdictions contrary to law.
- Information received from the Registrar General's Department indicates that, Mr. A provided different date of birth during the company incorporation process.
- Further intelligence revealed that Mr. A had earlier been convicted and jailed for eighteen (18) months in the United States of America for impersonation of a US Federal Official and visa fraud.
- Mr. A pleaded guilty to illegally using US Congressman's stationary and signature stamp in a series of attempt to obtain visas to the United States for people from his native country.

Indicators/ red flags

- Use and placement of large amount of cash into the financial system.
- Connivance with Ghanaian nationals.
- Unknown source of funds.
- Use of forged signatures and stamps of other persons.
- Previously convicted persons involved in other types of crimes.

5.1.7 Typology 7: Insurance Fraud

False Death Claim

Case Study 7.1

- The FIC received an STR filed by a Life Insurance Company K from the General Manager, Mr. Q of Company B regarding the death of Mr. G.
- As part of due diligence, the Life Insurance Company K noted that, all the documents presented by Mr. Q were fake.
- Mr. Q was further requested to provide the Medical Certificate of the cause of death and Police report but he was unable to present it to the Life Insurance Company K.

- Mr. Q further threatened to report the Life Insurance Company K to the regulator regarding the delay in the payment of death benefit.
- Further investigations conducted by the Life Insurance Company K revealed that the website, purported deceased's ID card and physical location of Company B were not in existence.
- Mr. Q did not pursue the claim further following interrogation by the Life Insurance Company K.
- The case was referred to the Law Enforcement Agency for investigations.

Indicators/ red flags

- Use of forged documents.
- Inability to present relevant documents.
- Loss of interest to pursue the death claim.

False Hospitalization Claim

Case Study 7.2

- The FIC received an STR in which a Client D of an insurance Company made a false hospitalization claim.
- An Insurance Company received a hospitalization claim for thirty (30) days from Client D purporting to have been admitted for the period.
- During an investigation conducted by the Insurance Company, it was revealed that, Client D was admitted for three (3) days and not thirty (30) days as earlier indicated.
- The case was referred to the Law Enforcement Agency for investigations.

Indicators/ red flags

- Use of forged documents.
- Fraudulent hospitalization claim

False Fire Insurance Claim

Case Study 7.3

- The FIC received an STR in which a Client P of an Insurance Company T made a claim on his car which supposedly caught fire.
- On June 22, 2017, Client P purchased an insurance policy valued at GH¢210,000.00.
- On September 28, 2017, Client P made a claim for payment with the Insurance Company U alleging his vehicle caught fire.
- Insurance Company T suspects that Client P's vehicle might have been stolen and the loss staged to get rid of the vehicle.
- Investigations is ongoing.

Indicators/ red flags

- Vehicle valued at high price to insurance company.
- Misrepresentation of facts to make claim.

5.1.8 Typology 8: Securities fraud

Investment Fraud

Case Study 8.1

- On October 7, 2017, the FIC received an STR from an Investment Company R for fraudulent transactions involving Ms. F and her Investment Broker W.
- Ms. F made an investment with Investment Company R through Investment broker W.
- On April 24, 2017, Ms. F made a fixed deposit of GH¢10,000.00 and GH¢54,000.00 with Investment Company R and withdrew all the funds after a number of rollovers.
- On July 6, 2019, a representative of Ms. F approached Company R and presented investment certificates purportedly issued by Company R.
- During investigations, Company R observed that some of the documents presented by the representative of Ms. F were forged.
- Further intelligence revealed that Ms. F had earlier contacted Company R to confirm whether the funds were with Broker W or the Investment Company R.
- Mr. T, a staff of Broker W misrepresented himself as a staff of Investment Company R to Ms. F.
- The matter is being investigated by the regulator.

Indicators/ red flags

- Use of forged and misleading disclosure documents.
- Misrepresentation of client to the investment company.
- Misrepresentation of a broker dealer in the transaction.

Frequency of funds used for investment

Case Study 8.2

The FIC received an STR from an Investment Company L on the frequency of deposits by a student.

- On December 15, 2017, Company U received a total investment deposit of GH¢47,000.00 within a week from a student.
- The student had previously worked with a Savings and Loans Company thereby arousing the suspicion of the student.
- The matter is being investigated by the regulator.

Indicators/ red flags

- Unknown source of funds.
- Use of forged documents.
- Inconsistency in the profile of client.

6.0 Conclusion

This typology report covers several schemes employed by criminals to commit various predicate crimes within the financial sector for the period under review.

The report further describes the various schemes and highlights all the red flag/ indicators to deepen understanding of Accountable Institutions and to further enhance the reporting of suspicious transactions to the FIC.

The FIC will continue to observe trends and patterns of money laundering activities and provide guidance through the development of typologies to Accountable Institutions, Law Enforcement Agencies, Policy Makers and the General Public on the future occurrences within the financial sector.

7.0 Recommendations

In order to combat and prevent money laundering and to take profit out of crime, Ghana may have to adopt the following measures:

- The FIC and relevant stakeholders to focus its activities in accordance with the risks identified in the NRA so as to increase understanding of the money laundering risks in the various financial institutions in view of this typology exercise.
- Law Enforcement Agencies to make use of parallel investigations in all money laundering investigations. An effective analysis of financial information by the FIC would go a long way to complement investigations of predicate offences.
- The Registrar General's Department should ensure the implementation of the beneficial ownership register and enhance access to it by relevant competent authorities.
- Stakeholders in the fight against Money Laundering should facilitate engagements with the private sector.

Design & Print



0264643339 | placardcommunications@gmail.com