# A CONCEPTUAL FRAMEWORK FOR DETECTING FINANCIAL CRIME IN MOBILE MONEY TRANSACTIONS

***Cross Gombiro*, Mmaki Jantjies*, Nehemiah Mavetera****

**Abstract**

Mobile money has made it possible for the unbanked to access financial service to areas previous not accessibly to traditional banking systems. Africa in particular, has indeed seen a growth in use of such services owing to the high penetration of mobile phones. While traditional banking services have been well regulated and secured, mobile money services are still new and vulnerable. Also, attacks and crimes targeting the internet, new technologies and new methods of payments have become sophisticated. This scenario requires novel proactive, real time techniques and solutions to detect financial crimes in mobile money transactions (MMT). The Financial Action Task Force (FATF) 2012 requires mobile money to be subject for monitoring and for compliance. Payment systems have evolved from hard cash, to credit cards, debit cards and now to the M-money, there are several approaches that have been used to detect financial crime in platforms such as credit cards and in the traditional banking system. However, most of these approaches are not suitable for m-money methods. A conceptual framework for detection of mobile money financial crime is proposed. The framework incorporates data mining techniques, big data analytics, Know Your Customers, historical databases and a knowledge base among other things.

**Keywords:** Mobile Money Transfer, Financial Crime, Tax Evasion, Financial Inclusion, New Methods of Payment

**Faculty of Commerce & Administration, Private Bag X2046, Mmabatho, 2735, North West University, South Africa*

## 1 Introduction

Mobile money is a new payment systems phenomenon especially in the developing world. Mobile money (M-money) is the process where products with monetary value are transferred (wired) electronically between one or more recipients, the sender and the receiver. Mobile cash is just but one of the examples of M-money. Coupled with a large number of population not having bank accounts, Africa has seen a tremendous growth in adoption and embracing of M-money. M-money services sometimes called Digital money has in it some risks just like other electronic platforms (e-platforms). The e-Platforms have become a playground of cyber-criminal, phishing and other financial crimes.

Financial crime falls under category of financial abuse crime where the crime perpetrated is not violent in nature but result in loss of finances. Financial crime involves among others tax evasion ,money laundering among others (Boorman and Ingves, 2001).

M-money is attractive to the criminals because of the following risks

- speed at which funds are transferred
- lack of physical contact
- ability of layering multiple transactions in small margins

Based on the stated risks above the approaches to counter money laundering ,terrorism financing is still in its infancy (Malady et al., 2014). Risks in M-money pose a challenge both on technology and access to banking services. There are risks posed with security of data, money laundering and financial fraud that need to be managed (Realini, 2011). According to Hamblen (2010), in Gartner report, fraud detection tools for mobile commerce are lagging behind, Fraud detection tools that work in wired networks do not work well in mobile world .Tools for detecting fraud in mobile spaces are still in the infant stages of development. There is need to explore the various approaches of countering financial crime and propose a new method of countering the traditional and emerging threats in the new methods of payment. An increasing market for M-money transactions result in an increase in risks involved. Mobile money transactions have become a target for both motivated and skilled attackers. M-money is vulnerable for abuse in areas such as money laundering. There is overwhelming data that makes it difficult to spot frauds in a timely manner(Coppolino et al., 2015a).

Financial crimes are continuously on the rise due to the ever evolving rise of technologies and new payment platforms such as M-money. M-money transfer refers to use of virtual money in payment of services through M-money. These services have increased especially in developed countries where most of the people are underbanked (Coppolino et al., 2015b). According to Lopez-Rojas and Axelsson

(2012),research in M-money fraud is not as advanced as in other fields. Also, M-money must be protected from money laundering.

This paper discusses M-money as new methods of payment. M-money, it further discusses methods used for money laundering and, methods used by authorities to detect and monitor financial crime using information technology. Limitations of current financial crime detection techniques are pointed out as well as the need for a new framework for M-money transactions monitoring and control. A review of existing frameworks is used to come up with a proposed conceptual framework for detection of M-money transactions (MMT). The rest of the paper is structured as follows: the remainder of Section 1 discusses characteristics of M-money applications, origins of risks involved in M-money and the M-money ecosystems. Section 2 delves into approaches that can be used in M-money financial crimes. Section 3 presents the conceptual framework for M-money financial crime detection and on Section 4, some reflections and conclusion are presented.

### *1.1 M-money application services characteristics*

M-money services have been broken into three parts by Solin and Zerzan ( 2010).These are i)What type of service they are ii) How these services are used and iii) an environment description in which these M-money services are used. Most of the services offered for M-money are for payment services in the following areas:

- Domestic and International transfers where parties in the same country transfer funds and regional money transfers between migrant workers and family members respectively.
- Storage of funds-other kind of payments involves storage of funds through an account.
- Retail payments for goods and services and payment of salaries (Solin and Zerzan, 2010).

### *1.2 How M-money crime risk can arise*

According to Chatain et al.(2008) anonymity, elusiveness, rapidity and lack of oversight are basically four ways in which M-money crime can be committed.

*Anonymity* – is done when a customer is unregistered or done when customer does not have the particulars to conduct a M-money transaction. The perpetrator can also use unregistered SIM card.

*Elusiveness* – One single account can be used in a community through a single individual through pooling. Normally various recipients receive money through one account in a many-to -one type of transactions or, through a rich person delegating a subordinate to do transactions on behalf of the boss. It is difficult to check such an account as the transactions can match with the profile of the rich boss.

*Rapidity* – M-money transactions can be done with speed, opening opportunities for layering hence a "would be criminal" can conduct several transactions in small amounts but to various recipients in a short space of time.

*Lack of oversight* – Happens when governing bodies are lax in the way they regulate M-money to such an extent that the platform is open for abuse through layering and transfer of money with no transaction cap (Chatain et al., 2008).

### *1.3 M-money Ecosystem*

The mobile ecosystem as described by Tobbin (2011) has various players that include partner banks, Mobile Network Operators(MNO), Regulators, Merchants, Consumers and distribution channel .The players involved in M-money ecosystem include MNO, Banks and regulators. The MNO provide the facilities and distribution channel for subscribers to conduct M-money transactions. Mobile Network Operators work in conjunction with agents (distributors) to do business on behalf of them. There are also merchants that are involved in remittances. Distribution channels normally act as point of contact with the customers that are involved with customer registrations and cash in cash services (Tobbin, 2011).

Banks are also part of the ecosystem as they store customer deposits in trust accounts. They also provide online banking integration to the mobile commerce (m-commerce) systems. They are also there to provide financial regulatory advice to MNO. Merchants and utilities also are involved in the M-money ecosystem. They include retail shops, lottery, casinos, goods and service provides where they use the system for receiving payment from customers for which Digital Subscriber Television (DSTV) and Electricity payments are typical examples.

## 2 Approaches for dealing with financial crime in M-money transactions

Most of the approaches dwell on data mining approach for Anti Money laundering. The frameworks studied touch most on traditional banking and on credit card fraud. Very few frameworks dwell on M-money as it is in its infancy. However from the materials searched on peer reviewed journals there are some concepts that can be learnt from traditional banking systems and the methods used for detecting financial crime. The Financial Action Task Force (FATF) formed in 1989 came up with rules governing financial crime in the Banking sector. These recommendations have continuously been revised as criminals come up with new methods for countering set procedures. The most recent revisions are the FATF 2012 recommendations. The recommendations do encourage using policies to deal with crime risk in financial domain. There are also recommendations for Know Your Customers (KYC), Employees and

Knowing Your Customer's Customers. However it is upon countries to embrace these FATF guidelines and recommendations.

### *2.1 Money laundering detection framework*

Mehmet et al., (2013) in their research. "Money laundering detection framework to link the disparate and evolving schemes" developed a detection framework for money laundering.

The framework provided covers many financial services including electronic money (E-Money) for detection using algorithms and suspicious trail databases. This might be helpful as the research questions also point to how one can identify suspicious transactions. This is also useful for fraud detection and money laundering. However the above framework is a large framework covering many aspects including M-money. In our framework we are only scaling down on M-money and not covering other monetary transactions such as traditional banking. We extract some of the components for use in our framework.

### *2.2 Fraud profiling conceptual model*

Brungs et al. (2008) , in their paper "Developing a Conceptual Framework for Identity Fraud Profiling" came up with a framework for identifying fraud through profiling. Their framework looks at profiling methodology through some notification and message passing to some modules. There are some policies that monitor activities, monitor profiles together with biometric biography, identity data, PINs and key loggers. Some concepts of profiling can be useful in our framework as it helps eliminate the risk of anonymity and helps to enhance Know Your Customer (KYC) and Customer Due Diligence (CDD).

### *2.3 Data Mining Framework for Financial Accounting Fraud Detection*

The framework for the detection of financial accounting fraud was proposed by Sharma and Panigrahi (2013). This framework explores the data mining method that can be used in financial statement and accounting frauds. The framework was mainly designed for detecting outliers and visualization for finding rare patterns. The assumption on their framework was that outlier detection techniques are suitable for distinguishing fraudulent data from authentic data, the techniques for visualization has the ability to present data anomalies. The framework design suits traditional banking model but some of the techniques can be used in M-money especially the outlier detection technique. However, care should be taken as criminals can use smurfing method to circumvent outlier detection by using below threshold values to transact various amounts to many customers. This technique has to be combined with other techniques for it to work in the presence of emerging new payment methods.

### *2.4 Multi-Variant Relational Model for Money Laundering Identification using Time Series Data Set architecture*

An architecture for money laundering was proposed by MCA and Prabakaran (2014) for the detection of laundering proceeds using multi variant model based on transaction set.

The architecture describes pre-processing of transaction data log by removing incomplete log data. These data transactions have to be checked through relational mapping by separating distinct from unique accounts. The accounts data is checked for one to many relational metric. The retrieved patterns from the log are then converted into a generalized format. The data that has been converted is then forwarded for money laundering identification. In the money laundering identification, a time series data of the transaction data will be performed by splitting data performed at a particular time frame. There is then a computation of overall amount transferred from one to many or many to one relationship based on to threshold values. A rule set is done to check if total transaction done surpass the total threshold for it to become a suspicious transactions(MCA and Prabakaran, 2014).

What is valuable from the framework in our research is the one-to-many or many-to -one transactions detection. It can be used to detect criminals that use mules or those that break larger transactions into smaller chunks. Again a criminal can deposit money into one's account and forward it to a transaction chain where the mine will come back to the criminal as legal money. Criminals such as those who dupe people into pyramids or multi sales of house to many home seekers can be detected in this many-to-one type of financial fraud.

### *2.5 A Monitor for Detecting Money Laundering and Terrorist Financing*

This framework was proposed by Helmy et al. (2014). It is used for detecting and monitoring transactions that might be showing signs of deviation from set rules for legitimate transactions. In the framework the system checks for customer risk and attaches a risk on transaction by placing a severity degree. The transaction is monitored in rule base, cycle detection and clustering modules. If one of the modules detects that the transaction is suspect then the transaction is given a risky score and marked as suspect. The transactions are then displayed according to their risky score in tabular format.

The transaction passes through the monitoring phase which contains many modules such as rule base,

feature detection, cluster, cycle detection, and suspected link monitors. The framework proposed assigning risk to customer and transactions due to Customer's due Diligence.

They proposed that, if a customer wires money to a suspect, then it is deemed suspect through a suspect link analysis by under covering hidden relationships such as a sanction list person or any person informed by government. The framework also provides for cycle detection where money transferred through layering is returned back to the initiator. Any transaction deemed suspect is checked in the history databases. The importance of this framework to our proposed framework is that we can make use of suspect link analyser and assign customers a risky level. For example, previously convicted offenders can be assigned risky customers status, and any transaction they conduct is deemed suspect. Cycle detection can also be used in our framework to detect suspects that want to introduce illegal money and withdraw it as legitimate money.

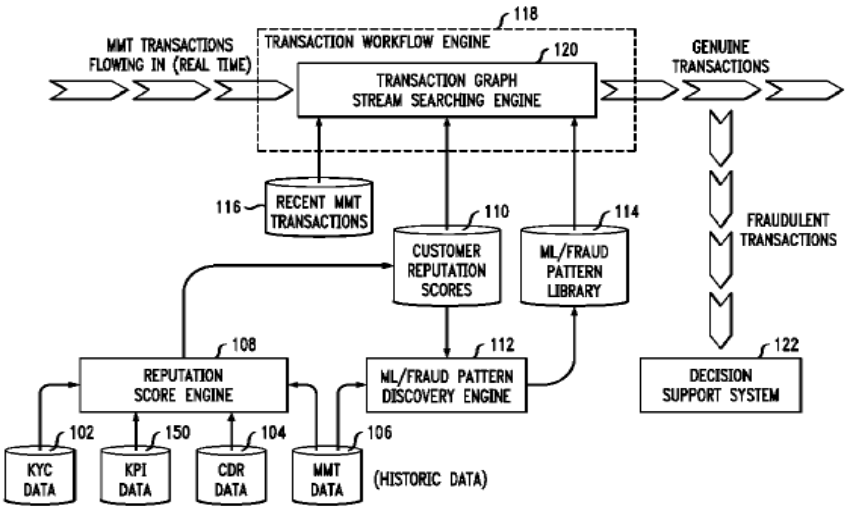
### *2.7 Framework of Data Mining System for Anti money Laundering*

A framework using data mining for anti-money laundering was proposed by Luo (2014) where transactions are cleaned and transformed for data mining and discovered knowledge is put into a knowledge base which can be used for visualisation and recommender systems. The framework focused on dynamic detection mechanism for suscipicious transactions using stream data using classification based algorithm.The framework is not well suited to M-money ecosystem based at the speed at which the transactions are performed. However, knowledge base for keeping the discovered knowledge might be usefull in our proposed framerwork.

### *2.8 Detecting fraudulent M-money transactions*

Figure 1 details a framework for detecting fraud in M-money transactions.

**Figure 1**. Framework for detecting fraudulent M-money transaction adapted from




Source: Batra et al., 2013

The framework by Batra et al.(2013) , was designed to define a reputation score based on historical data, use reputation to determine multiple patterns related to fraudulent M-money transfer, detect customer patterns and classify transaction as genuine or fraudulent.The framework attempts to identify fraud in real time by identifying potential risks through detecting anomolous M-money transfer transactions. The framework provides anomaly detection systems for identifying suspicous transactions in real time.The framework provides automatic detection patterns of money laundering in automated manner.The framework also provides Know your Customer database and call details records and inactive patterns.The framework also includes key perfomance indicators to measure customer usage pattern and automatically classifies transactions likely to be deemed suscipicious for money laundering.The data is then ranked through a reputation score database and customer reputation score for detecting money laundering (ML) or fraud pattern. These are then analysed through a transaction graph(Sun et al., 2006).The framework does not however provide ways on how to seperate fraudulent transactions from genuine transaction. This framework is useful in the development of our proposed framework as it can be used for setting rules and assignment of risk score in the ontology module.The historical database engine is also applicable in our framework as it is useful for keeping transaction records in accordance to FATF 2012 recommendations of keeping records for five years.

### *2.9 Analysis of the existing frameworks*

Most of the frameworks anlaysed use data mining ,but use of data mining has problems of uncovering only what the analyst are looking for and patterns identified may be a result of data inconsistence based on random fluctuations (Zengan Gao and Mao Ye, 2007).This can be addressed through big data analytics as use of data mining is human intensive and cannot cover data in motion effectively. Traditional fraud detection methods sorely focused on identification, verification and profiling of customers using historical transactional data However, according to Zengan Gao and Mao Ye (2007), they are weak in uncovering potential fraud and insider trading. Data mining has its own challenges such as noisy data, difficulties of tracing user behaviour and also, behaviour changes quite frequently. In addition, extracting large volumes of data need high efficient techniques (Singh and Singh, 2015).

## 3 The need for a new framework

Basing on the various methods and frameworks for detecting financial crime in M-money, the imaging challenge calls for a holistic approach to uncover hidden risks in M-money. Tackling financial crime is a challenge because a lot of internal control systems have serious control weaknesses. However, its key aspect is the ability for technology to maintain comprehensive logs of all performed activities and electronic transactions of fraudulent activity or heightened fraud risk (Dzomira, 2014).

Cyber criminals know that banking financial detection systems rarely monitor behaviour of customers across multiple accounts, channels and systems and this weakness opens the door for cross-channel financial crime. In this process, a fraudster gains access to customer information in one channel and uses that to commit fraud through another. Also, the anonymity of e-commerce makes it more difficult to uncover bogus communications and hidden relationships (Joyner, 2011).

### *3.1 Proposed Conceptual framework for M-money financial crime detection*

Money Laundering (ML) patterns and the networks for purported ML is essential for automated ML but focus in traditional research has been on legislation and compliance. The methods are limited to incident identification, suspicious surveillance avoidance detection with investigations being manual, tedious and somewhat resource intensive as well as time consuming. The current methods do not address false positive rates well and become invalid in the presence of high volume sets (Zengan Gao and Mao Ye, 2007). In our proposed framework we take this into account through the use of big data analytics where the method looks at large volume of data and deals with variety and removal of noisy data. The velocity of the data (real time environment and the speed at which the data is generated) .Based on the millions of transactions generated by M-money transactions, there is need to extract value from the data. Identification of legal transaction as an illegal transaction can result in lawsuits while identification of an illegal transaction as legal can result in loss of business and promotion of money laundering and financial crime practices.

#### *3.1.1 Discussion of the framework*

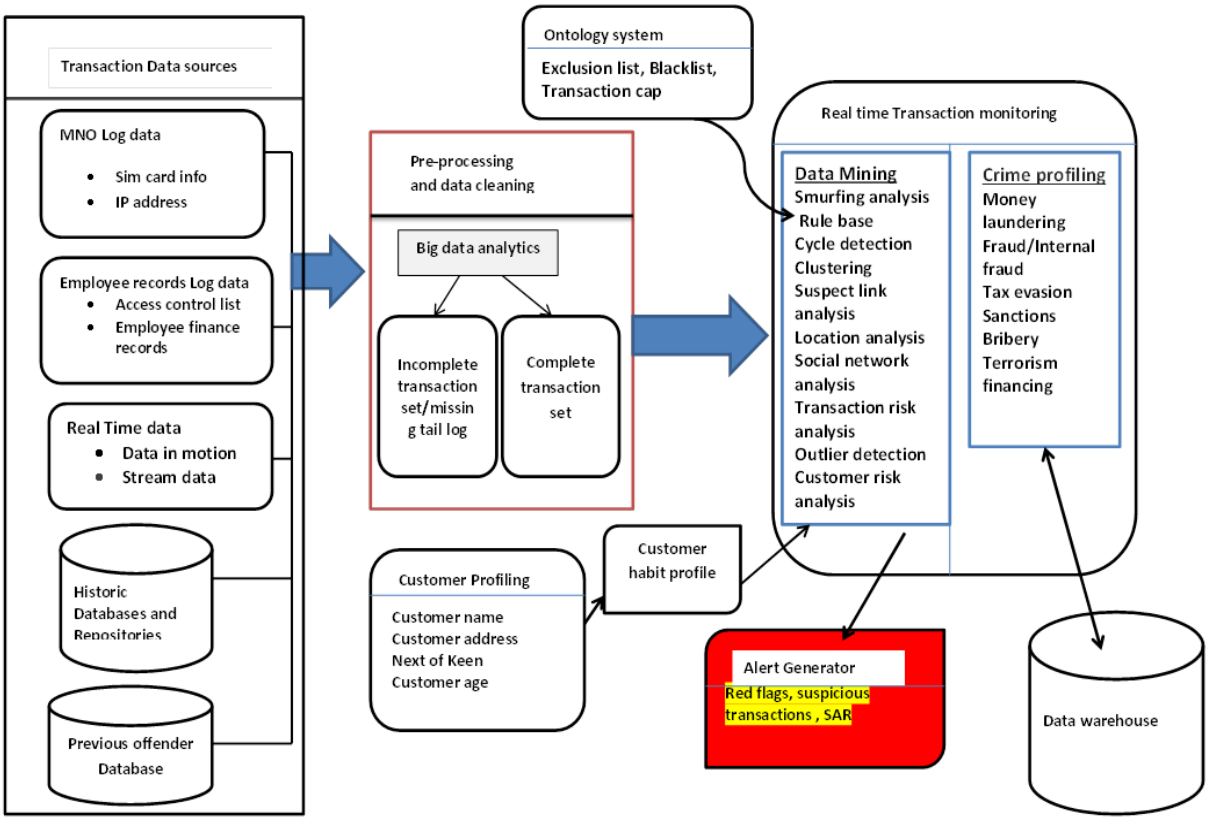
Figure 2 presents the proposed conceptual framework for detecting M-money financial crime. The framework encompasses monitoring activities such as fraud, social network analysis,and money laundering.The framework also encompasses the FATF 2012 recommendations and preliminary observations through the use of M-money platforms and their requirements.The dynamic nature of financial crime needs a holistic approach to help Financial Intelligent Unit (FIU) and investigating officials to detect financial crime by using automated approaches. Care should be taken to correctly identify suscipious transactions when a transaction deemed suspect is not suspect or one deemed clean is suspect. Our framework can be used for helping investigators and FIU to discover hidden traits in M-money transactions.

#### *3.1.2 Transaction data sources*

The framework will use various sources of information for data processing. The different data will be put in an XML for pre-processing and cleaning. XML files are not database specific, they convert files to a standard format. The data originates from mostly log files from MNO that have records such as SIM card, SIM card replacement information and the SIM registration information. Though most of agent data will be generated on the MNO's network, the data will be kept on MNO databases. This information will be used for pre-processing. Employee records data will be used for the sessions they logged in and their access rights. Employee data could also include their financial worth and declarations of what they own.

Transaction data in motion will also be subjected for data cleaning where successful and failed transactions will be cleaned for processing. Historical data and repositories contain committed transactions and past transaction records. The FATF requires that banks and financial institutions should keep transaction data for a period of not less than five (5) years. Previous offender database will contain a list of offenders who have been previously convicted or warned on financial crime. This includes persons that have been blacklisted in the banking sector and persons previously suspected of financial crime but won the cases.

**Figure 2.** Conceptual framework for detection of M-money financial crime




### *3.1.3 Pre-processing*

The data gathered form data collections will be cleaned to check for incomplete and noise transactions. Big data analytics tools can be used since the data might be in motion as well as the data being voluminous. The transactions that are complete are then forwarded for monitoring

### *3.1.4 Ontology System*

Ontologies are domain related intensional models and developed to capture information or knowledge that need to be shared (Mavetera and Kroeze, 2010). Knowledge is represented in declarative formalism with sets of objects describing relationships among them(Gruber, 1995). Ontology can also be regarded as a knowledge-based system that uses a declarative knowledge base containing the concepts and the relations that exist in a given domain(Trausan-Matu and Neacsu, 2008). Rules for setting threshold values, exclusion list, and transaction cap can be set in an ontology module for use during the transaction monitoring. Rajput, et al.( 2014) state that " Ontology is used to develop an expert-system as it provides an unambiguous specification of knowledge and is adaptive in case of dynamic knowledge base. The ontology-based expert system consists of domain knowledge as well as some rules to support reasoning". This module will be helpful for the rule base and, outlier detection and link analysis. The sets for exclusion list, customer ranking and outlier detections are specified in the ontology engine. The set rules for identifying genuine and suspicious transactions are specified in the ontology system engine.

### *3.1.5 Real Time transaction monitoring*

Most of the detection tools and methods are passive in nature .In this proposed framework the module checks for suspicious transactions in real time .The data mining techniques can be used for checking various offences through clustering, suspected link analysis, location analysis where the system checks for geographical location of the suspect and customer habits. If a transaction is deemed suspect, it will be profiled depending on probabilities of the variable and rank. For example a many-to-one transaction might indicate a commission of fraud such as pyramid fraud or a housing agent selling a single house to many persons. For any transaction conducted and linked to a blacklisted person, the said transaction will be categorized as suspect.

### *3.1.6 Alert Generator*

When the system is monitoring the transactions, and if there is probability that a transaction is suspect, then, it is sent to the alert generator for red flags and suspicious activity report.

### *3.1.7 Customer Profiling*

This will be used for Know your customer policies and Customer Due Diligence .The profile information can help in understanding customer habits and social network analysis. The link analysis can be used to analyze interaction behaviour patterns, identify suspect links and uncovering hidden groups.

### *3.1.8 Data warehouse*

Since information generated from monitoring is voluminous, it is best to store the information in a data warehouse for further analysis. The data warehouse is necessary to store heterogeneous data sources as well as being used for inferring data through use of Dempster-Shafer theory. The theory is also used for combining evidence(Yager, 1987;Panigrahi et al., 2007).The theory can be used to avoid unwanted results for example seperating genuine from illegal transactions in the proposed framework (Coppolino et al., 2015a).

## 4 Reflection and conclusion

Our framework uses data cleaning, pre-processing and use of historical databases. Suspicious data come from employee logs, historical offenders' database and historical and real time transaction data. The flags and Suspicious Activity Reports (SAR) are forwarded for analysis by crime analysis agency for further analysis. Ontology is set to define a set of rules to link customers, customer ranking, threshold values and transaction rules. The problem of identifying anomalies in MMT is a challenge. However, the framework addresses the problem by use of various data mining approaches as well as the use of Dempster Shafer theory to identify evidence of financial abuse and assign probabilities based on likelihood of transaction to fall under illegal transaction. What can be added for further research is including geographical location analysis and algorithms for faster execution of the identification and execution of the tools. There is need to uncover and continuously update the rule base as criminals always come with new techniques in money laundering, cybercrimes and other financial crimes

## References


1. Batra, V.S., Garg, D., Kothari, R., Krishnapuram, R., Negi, S., Parija, G.R., 2013. Detecting fraudulent mobile money transactions. US8458090 B1.
2. Boorman, J., Ingves, S., 2001. Financial system abuse, financial crime and money laundering-background paper. Wash. IMF.
3. Brungs, A., Winchester, D., Stephens, G., Smith, S., 2008. Developing a Conceptual Framework for Identity Fraud Profiling.
4. Chatain, P.-L., Hernández-Coss, R., Borowik, K., Zerzan, A., 2008. Integrity in Mobile Phone Financial Services. World Bank Work. Pap.
5. Coppolino, L., D'Antonio, S., Formicola, V., Massei, C., Romano, L., 2015a. Use of the Dempster-Shafer Theory for Fraud Detection: The Mobile Money Transfer Case Study, in: Intelligent Distributed Computing VIII. Springer, pp. 465–474.
6. Coppolino, L., D'Antonio, S., Formicola, V., Massei, C., Romano, L., 2015b. Use of the Dempster–Shafer theory to detect account takeovers in mobile money transfer services. J. Ambient Intell. Humaniz. Comput. 1–10.
7. Dzomira, S., 2014. Digital forensic technologies as e-fraud risk mitigation tools in the banking industry: evidence from Zimbabwe. Risk Gov. Control Financ. Mark. Inst. 4, 116.
8. Gruber, T.R., 1995. Toward principles for the design of ontologies used for knowledge sharing? Int. J. Hum.-Comput. Stud. 43, 907–928.
9. Hamblen, M., 2010. Mobile commerce growth outpaces anti-fraud tools, Gartner says [Online]. Computerworld. URL http://www.computerworld.com/article/2515612/mobile-wireless/mobile-commerce-growth-outpaces-anti-fraud-tools--gartner-says.html (accessed 6.21.15).
10. Helmy, T.H.E., Abd-ElMegied, M. zaki, Sobh, T.S., Badran, K.M.S., 2014. Design of a Monitor for Detecting Money Laundering and Terrorist Financing. Int. J. Comput. Netw. Appl. 1, 15–25.
11. Joyner, E., 2011. Detecting and preventing fraud in financial institutions.
12. Lopez-Rojas, E.A., Axelsson, S., 2012. Multi agent based simulation (mabs) of financial transactions for anti-money laundering (aml), in: Nordic Conference on Secure IT Systems. Blekinge Institute of Technology. p. 94.
13. Luo, X., 2014. Suspicious Transaction Detection for Anti-Money Laundering. Int. J. Secur. Its Appl. 8.
14. Malady, L., Buckley, R.P., Arner, D.W., 2014. Developing and Implementing AML/CFT Measures Using a Risk-Based Approach for New Payments Products and Services. CIFR Pap.
15. Mavetera, N., Kroeze, J.H., 2010. An ontology-driven software development framework.
16. MCA, G.K., Prabakaran, M., 2014. An Multi-Variant Relational Model for Money Laundering Identification using Time Series Data Set. Int. J. Eng. Sci. 3, 43–47.
17. Panigrahi, S., Kundu, A., Sural, S., Majumdar, A.K., 2007. Use of dempster-shafer theory and Bayesian inferencing for fraud detection in mobile communication networks, in: Information Security and Privacy. Springer, pp. 446–460.
18. Rajput, Q., Khan, N.S., Larik, A., Haider, S., 2014. Ontology Based Expert-System for Suspicious Transactions Detection. Comput. Inf. Sci. 7.
19. Realini, C., 2011. Securing Mobile Money to Deliver on the Promise. Lydian J.
20. Sharma, A., Panigrahi, P.K., 2013. A review of financial accounting fraud detection based on data mining techniques. ArXiv Prepr. ArXiv13093944.
21. Singh, P., Singh, Mandeep, 2015. Fraud Detection by Monitoring Customer Behavior and Activities [WWW Document]. URL (accessed 6.21.15).
22. Solin, M., Zerzan, A., 2010. Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks. GSM Assoc. Last Modif. January.
23. Sun, L., Srivastava, R.P., Mock, T.J., 2006. An information systems security risk assessment model

under the Dempster-Shafer theory of belief functions. J. Manag. Inf. Syst. 22, 109–142.
24. Tobbin, P., 2011. Understanding mobile money ecosystem: ROLES, structure and strategies, in: Mobile Business (ICMB), 2011 Tenth International Conference on. IEEE, pp. 185–194.
25. Trausan-Matu, S., Neacsu, A., 2008. An ontology-based intelligent information system for urbanism and civil engineering data. Concept. Models Urban Pract. 85–92.
26. Yager, R.R., 1987. On the Dempster-Shafer framework and new combination rules. Inf. Sci. 41, 93–137.
27. Zengan Gao, Mao Ye, 2007. A framework for data mining-based anti-money laundering research. J. Money Laund. Control 10, 170–179. doi:10.1108/13685200710746875