American Journal of
Accounting
(AJACC)

EFFECT OF CASH TRANSPORT ON THE FINANCIAL PERFORMANCE OF COMMERCIAL BANKS IN KENYA

Mactosh Onwonga, Prof. George Achoki and Dr. Bernard Omboi

American Journal of Accounting
Vol.1, Issue 2 No.1, pp 16 - 35, 2017
www.ajpojournals.org

EFFECT OF CASH TRANSPORT ON THE FINANCIAL PERFORMANCE OF COMMERCIAL BANKS IN KENYA

[1*] Mactosh Onwonga
[1]Post Graduate Student: United States International University
[*]Corresponding Author's E-mail: mactoshonwonga@gmail.com

[2]Prof. George Achoki
United States International University

[3]Dr. Bernard Omboi
United States International University

Abstract

Purpose: The main aim of the study was to assess the effect of cash transport on the financial performance of commercial banks in Kenya.

Methodology: The research was carried out through a descriptive survey research design. The study population was all the 43 commercial banks registered and licensed to operate in Kenya. A multi stage sampling approach was used. In the first stage, a census of all the 43 commercial banks was conducted, that is, the units of analysis were the commercial bank. In the second stage, purposive sampling was used where two respondents from every organization were taken. The study used both primary and secondary data for analysis. Primary data was collected using questionnaires while secondary data was obtained using secondary data collection template. A multiple linear regression model was used to link variables.

Findings: The study findings indicated a positive correlation between cash transport and financial performance of commercial banks. Cash transport was positively and significantly related to ROA. The study concluded that cash reconciliation is positively and significantly related to financial performance of commercial banks in Kenya,

Unique contribution to theory, practice and policy: The study recommends that commercial banks and other financial institutions involved in handling of cash should have a cash transport policy which clearly stipulates how cash in transit should be handled, regularly review the contracts of companies which transport cash for them so as to avoid known routines, have tracking devices in the vehicles that transport cash, engage administrative police in security arrangements when transporting cash and invest in cash in transit measures like chase cars. The study recommended further studies to establish the effect of cash handling practices on financial performance of other financial institutions other than commercial banks. This will be crucial in comparison of the results and identification of more research gaps for future studies.

Key words: *cash handling, cash transport, financial performance, commercial banks*

1.0 INTRODUCTION

Bank failures are as old as banking industry itself. Despite the significant roles it plays in economic development, its failures are becoming well pronounced. The Dictionary of Economics and Commerce confirmed that 200 banks failed in England between 1815 and 1850 just a period of 35years, one of the reasons attributed to this failure is fraud.

The problem of fraud in banking industry is not limited to any economy, nation, continent or an environment; it is a general phenomenon. The origin of bank failure in Nigeria can be traced to the 1930s bank failure and crises. Nwankwo (1994) wrote that "the crises of confidence in Nigerian banking industry is not a new one, it has been with us for quite a long time. It occurred in the1930s when all indigenous banks, except one (National Bank), collapsed. It occurred again during the banking 'boom and crash' of the late 1940s when all but four indigenous banks escaped the liquidators hammer". Also between 1952 and 1954, 16 out of 21 indigenous banks failed. In the late 1990s, 26 failed banks were liquidated at once while others went through various surgical operations ranging from, restructuring, renaming, acquiring and complete sales to new investors. One thing that is constant in all the reforms was that fraud was a prominent factor in major failures.

Fraud as a result of cash mishandling has become a major source of concern for Banks in Kenya. The media is awash with news of how banks are losing billions of shillings every year to fraudsters. While not all fraud losses are reported, figures from the Banking Fraud and Investigations Department (BFID) of the Central Bank of Kenya indicate that significant amounts are actually lost by banks each year in this country. Money is lost due to loopholes caused by poor cash handling practices by banks which leads to exploitation by the fraudsters. Cash is lost while under storage, when in transit or through theft by bank employees who take advantage of the poor cash reconciliation practices put in place. The recouping of the lost amounts is improved when the losers have better cash insurance measures in place. According to Mbuguah (2013), the net outcome of these huge losses is poor performance. For listed banks this could lead to a drop in the value of their shares or more stringent oversight /control by their multiple regulators. For both listed and non-listed banks, this leads to lack of trust from their customers hence they seek alternative banking institutions.

The Australian Institute for Criminology defines Cash-in-transit as the transport, delivery and receipt of cash using escort services like armored vehicles (Smith & Louis, 2010).The institute further defines Cash-in-transit (CIT) robbery as the unlawful and intentional forceful removal and appropriation of money or containers for the conveyance of money, belonging to another while such money or containers for the conveyance of money are being transported by a security company on behalf of the owner thereof. According to Van Anholt (2014), transportation or cash-in-transit involves picking up valuables and taking these valuables to designated points. This basic service still remains the largest revenue producer for most carriers even though cash management is closing the gap. Carriers utilize armored vans or trucks to transport valuables. Some carriers use vans when servicing ATM's or carrying lighter loads but a van chassis does not support the weight of coin or heavy currency loads. The cardinal rule in the cash-in-transit business is to always get and give a receipt.

The Basel Core Principles for Effective Banking Supervision states that 'Risk Management Processes' requires that banks and banking groups have comprehensive risk management processes (including Board and senior management oversight) to identify, evaluate, monitor and control or mitigate all material risks and to assess their overall capital adequacy in relation to their

risk profile. These processes should be commensurate with the size and complexity of the institution. The central bank of Kenya highly encourages the same through the Central bank of Kenya Risk management Act (2013).

The nature of risk involved in handling of cash is recognized by the Central bank of Kenya. The bank frequently circulates circulars encouraging the commercial banks operating in Kenya to adhere to requirements which has been highlighted in the Risk management Act (2013).The central bank of Kenya came up with guidelines which every bank should adhere to in order to reduce the risks involved with handling of cash. The risk management guidelines (2013) provided by the central bank of Kenya to the commercial banks states that the banking institutions should develop implement and maintain an enterprise-wide Operational Risk Management Framework that is fully integrated into the bank's overall risk management processes. Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. Such risk may include loss of cash as a result of failed internal processes, people and systems during CIT, storage or when reconciling various accounts. The guidelines states that the developed framework should have reporting lines and accountabilities, describe the bank's accepted operational risk profile and approved risk mitigation strategies and instruments and establish risk reporting and Management Information System (MIS). The risk management guidelines (2013) further highlights the procedures for determining whether and how activities can be outsourced.

Outsourcing of third party companies like security companies to offer CIT services and securing the storage area of funds should follow certain procedures indicated by the guidelines. The guidelines requires that the bank should clearly state the processes for conducting due diligence in the selection of potential service providers, sound structuring of the outsourcing arrangement, including ownership and confidentiality of data, as well as termination rights, programmes for managing and monitoring the risks associated with the outsourcing arrangement, including the financial condition of the service provider , Establishment of an effective control environment at the bank and the service provider , development of viable contingency plans and execution of comprehensive contracts and/or service level agreements with a clear allocation of responsibilities between the outsourcing provider and the bank. Despite the fact that there are guidelines relating to operations of the commercial banks concerning handling of cash, cases of fraud as a result of poor cash handling practices has been on the rise.

British Security Industry Association (2008) report indicates that with the downturn in the global economy, cash-in-transit (CIT) crime is on the rise. In the U.K alone, there is an estimated £500 billion being transported each year, or £1.4 billion per day. Money stolen in CIT attacks is a major source of funding for serious organized crime. The reports further states that in 2008 there were 1,000 documented attacks against cash-in-transit couriers in the UK. This is out of a total of 4,000 boxes in use throughout the year. The latest statistics from the British Security Industry Association show that attacks against cash-in-transit couriers remain a serious problem and the attacks and robberies are a pervasive and growing problem throughout the world.

According to research done by Smith and Louis (2010), United Kingdom (UK) has considerable risks in CIT robberies. In 2005 the UK had a total number of 763 reported cases of CIT robberies. In comparison with South Africa, the study found out that South Africa had 509 cases of CIT theft cases the same year. According to the Brazilian Federation of Bank, in 2009 the country lost $30 Million due to bank robberies and Cash-in-transit robberies (Smith, 2010). Febraban stated that

money stolen in a CIT robbery rarely exceed $300 000.00 but in some cases like an incident that happened on the 5th of November 2009 where a total of $4 Million was stolen (Smith, 2010). In Brazil 10% of all bank robberies are directed at armored vehicles and cash in transit (Smith, 2010).

Measures by G4S Security Company to try and fight the thefts of cash in transit are further proof of an increase in the vice. According to Njiraini (2010), the security company announced new measures to prevent theft of cash in transit. G4S was hit by a series of daring robberies in the subsequent years in which cash it was contracted to deliver was stolen while on transit. Among the new measures it has introduced is a stronger vetting process for both police officers and escorting cash vehicles, and its employees involved with cash-in transit. G4S will now carry out lie detection tests using polygraph machines, and increase supervision and security checks. It also plans to install its vehicles with satellite real time monitoring and controls devices, establish a new operating protocol with the police, and enhance staff training and compliance programmes. G4S also plans to introduce new cash centres, in collaboration with commercial banks, to reduce the distance which cash is in transit.

1.1 Problem Statement

Poor cash handling practices by commercial banks leads to massive losses ultimately leads to a negative performance and in extreme circumstances, closure of the commercial banks. The collapse of Royal British bank and City of Glasgow bank in the 18th century, Barings bank in the 19th century to the most recent collapse of Euro bank in Kenya in 2003 as a result of poor cash management attests to this apprehension (Grossman, 2010; Taylor, 2007). The rising cases of fraud as a result of poor cash handling practices in the Kenyan commercial banks since 2011 have been overwhelming. This is evidenced by recent cases of cash in transit being stolen by security firms contracted to transport the cash. According to Fayo (2015), G4S Security Company was involved in cash in Transit theft of cooperative bank of Kenya cash which was being transported from the bank's Maua branch in Meru to its Koinange branch in Nairobi.80 million was stolen in the process. The company has also been involved in other cases of theft with consolidated bank of Kenya. It had previously been ordered to pay 18.55 Million to consolidated bank for being involved in cash in transit theft. Ndonga (2014) states that theft of cash in transit is not only by the G4S security company but also other security companies contracted to transport it. A recent case involved KK security officers making away with a total of Sh82 million which they were transporting from Westlands to the Central Bank of Kenya. Despite the fact that the distance between Westlands and Central bank of Kenya was short, money is still being stolen. Poor cash transportation practices are to blame for that. Deloitte report (2013) states that companies, especially those dealing with huge sums of money like banks and supermarkets are ill-prepared to fight this onslaught, which is costing them millions of dollars annually arising from information security breaches and corporate theft. The study therefore sought to assess the effect cash transport on the financial performance of commercial banks in Kenya.

1.2 Research Objective

To assess the effect cash transport on the financial performance of commercial banks in Kenya.

2.0 LITERATURE REVIEW

2.1 Theoretical Review

2.1.1 Cash Management Theory

Cash management theory provides the process of planning and controlling cash flows into and out of the business, cash flows within the business, and cash balances held by a business at a point in time (Pandey & Jaiswal, 2011). According to the theory, efficient cash management involves the determination of the optimal cash to hold by considering the trade-off between the opportunity cost of holding too much cash and the trading cost of holding too little. The theory provides the process of planning and controlling cash flows in and out of the business. The theory informs the study as it will help to bring more understanding to the process of cash handling and test whether the firms subscribe to the guidelines provided by the theory. It will then be easy to link subscriptions to this guidelines and performance of the firm. The handling of cash is in itself a risk and the more inflows there is, the more risky it becomes hence proper measures should be put in place to curb the frauds.

The purpose of cash management is to determine and achieve the appropriate level and structure of cash, and marketable securities, consistent with the nature of the business's operations and objectives (Brigham, 1999). As Erkki (2004) asserts, models on cash balance management have been proposed by (as cited in Baumol, 1952), Archer (1966), Beranek (1963), Miller and Orr (1966), Pigou (1970), Lockyer (1973), and Gibbs (1976) among others. William Baumol (1952) was the first person to provide a formal model of cash management. As noted by Erkki (2004), this model applied the economic order quantity (EOQ) to cash. Brokerage fees and clerical work form order costs while foregone interest and cash out costs forms the costs of holding cash. Baumol's model is however probably the simplest, most striped down and sensible model for determining the optimal cash position (Ross, 1990; Lockyer, 1973) on the other hand modified Baumol's model to incorporate overdraft facilities. According to Lockyer's approach the total annual cash policy cost attributable to the use of overdraft facilities is given by the sum of total annual cash transfer cost, total annual overdraft cost and the total annual holding cost. Erkki (2004) further asserts that Lockyer's model is critiqued for assuming overdraft facilities, which are not automatic especially for firms with poor credit rating. The model also assumes disbursements are even over the planning period.

According to Erkki (2004), the cyclical nature of cash is recognized for reasons that apart from providing cash balance for transactional purposes, a cash balance should be provided for precautionary purposes, especially for seasonal activities that are unpredictable. In Archer's approach, costs related to overdraft facilities and capital costs of precautionary balances are compared to determine the optimum. Archer's approach is advantageous for it recognizes the cyclical nature of net cash flows of many firms. According to Gibbs, the determination of optimal cash balance involves a combination of investment and financial decisions. In Gibbs approach, cases where demand for money is of a cyclical nature a combination of short and long term borrowing should be used to avoid the use of long term funds to cover peaks arising from idle cash balance, during periods of low cash demand. Gibbs (1976) contends that, the determination of the amount of buffer money to hold is seen as an investment decision. Gibbs approach emphasizes holding costs, costs of short and costs of long-term borrowing and the costs of investment in marketable securities (Erkki, 2004).

In order to do this a variety of activities need to be undertaken, because of the integrative nature of cash to the operation of the bank. Since most of the bank operations revolve around advancement of cash then it is imperative for a considerable minimum level of cash to be maintained. How a bank manages cash will definitely have implications on the liquidity of the bank. The theory therefore is of essence on the bases of the policy the banks may have in place with regard to cash retention so as to avoid illiquidity.

2.1.2 Fraud Management Lifecycle Theory

The fraud management lifecycle effective management of the fraud management lifecycle starts with a common understanding or definition of the stages in the lifecycle. Without this awareness and understanding, fraud management professionals are unlikely to communicate effectively with each other, with their peers in other industries, and within their respective businesses. The terms "lifecycle stage" and "stage" throughout this document are used as a reference to a set of activities. The use of the term stage does, however, bring with it references to a series of sequential independent actions that is not representative of the concepts being advanced by this document. Webster's dictionary refers to a lifecycle as a series of stages in form and functional activity through which an organism passes between successive recurrences of a specified primary stage (Webster, 1997, 1976, & 1941).

Webster also refers to a network as "an interconnected or interrelated chain, group or system" (Webster, 1997, 1976, & 1941). The Fraud Management Lifecycle can be best described as a combination of these two definitions, a network lifecycle. Unlike a traditional linear lifecycle, a network lifecycle's stages are not necessarily linked sequentially, where activities in one stage are completed and then the functioning is passed on to the next stage in the chain. To the contrary, a network lifecycle facilitates simultaneous and sequential actions within each of the lifecycle stages or network nodes. The convenient term "stage" in a network lifecycle is more specifically a reference to the activities, operations, and functions performed. One can reasonably think of the various lifecycle stages as various disciplines within fraud management. The linking of the lifecycle stages as network nodes allows the representation of non-linear, non-sequential, even recursive activity. The interrelationships and interdependence of the stages or nodes can be explained without the restriction of the traditional sequential lifecycle stage progression. The Fraud Management Lifecycle is, therefore, a network lifecycle where each node in the network, each stage in the lifecycle, is an aggregated entity that is made up of interrelated, interdependent, and independent actions, functions, and operations. These activities can, but do not necessarily, occur in a sequential or linear flow.

The Fraud Management Lifecycle is made up of eight stages. Deterrence, the first stage, is characterized by actions and activities intended to stop or prevent fraud before it is attempted; that is, to turn aside or discourage even the attempt at fraud through, for example, card activation programs. The second stage of the Fraud Management Lifecycle, prevention, involves actions and activities to prevent fraud from occurring. In detection, the third stage, actions and activities, such as statistical monitoring programs are used to identify and locate fraud prior to, during, and subsequent to the completion of the fraudulent activity. The intent of detection is to uncover or reveal the presence of fraud or a fraud attempt. The goal of mitigation, stage four, is to stop losses from occurring or continuing to occur and/or to hinder a fraudster from continuing or completing the fraudulent activity, by blocking an account, for example. In the next stage, analysis, losses that occurred despite deterrence, detection, and prevention activities are identified and studied to

determine the factors of the loss situation, using methods such as root cause analysis. The sixth stage of the Fraud Management Lifecycle, policy, is characterized by activities to create, evaluate, communicate, and assist in the deployment of policies to reduce the incidence of fraud. Balancing prudent fraud reduction policies with resource constraints and effective management of legitimate customer activity is also part of this stage. An example is the requirement that any cash transaction over $10,000 be reported (Webster, 1997, 1976, & 1941).

Investigation, the seventh stage, involves obtaining enough evidence and information to stop fraudulent activity, recover assets or obtain restitution, and to provide evidence and support for the successful prosecution and conviction of the fraudster(s). Covert electronic surveillance is a method used in this stage. The final stage, prosecution, is the culmination of all the successes and failures in the Fraud Management Lifecycle. There are failures because the fraud was successful and successes because the fraud was detected, a suspect was identified, apprehended, and charges filed. The prosecution stage includes asset recovery, criminal restitution, and conviction with its attendant deterrent value (Webster, 1997, 1976, & 1941).

Stage One: Deterrence

Successful deterrence is the stopping of fraud before it happens. Deterrence or "to deter," is defined as, "to inhibit or discourage through fear; hence to prevent from action by fear of consequences" (Webster, 1997, 1976, & 1941). In the fraud arena we need to expand this definition to include the aspect of difficulty. Fraudsters tend to migrate toward the path of most anonymity and least resistance. Therefore, increasing the difficulty of committing the fraud effectively functions as an incremental increase in deterrence. For example, when conducting an online transaction, requiring address verification provides an incremental increase in deterrent value, because the perpetrator must know how to circumvent and defeat the verification process. Adding a component to the online transaction becomes a deterrent, as it makes the fraudster work harder. For the purposes of this study deterrence will be defined as: activities designed, through fear of consequences or difficulty of perpetration, to turn aside, discourage, or prevent fraudulent activity from being attempted. The aggregate nature of deterrence is implied; deterrence is not viewed as a monolithic whole, but rather an aggregation of activities with varying degrees of deterrent value.

Deterrent value is a summation of the deterrent contributions and detractions provided by each stage in the Fraud Management Lifecycle. Thus, successful deterrence is contingent upon the performance of the other stages of the Fraud Management Lifecycle.

Stage Two: Prevention

In the fraud arena, prevention, detection, and deterrence are sometimes used synonymously. This contributes to confusion within the organization, as well as in external entities, about the focus of prevention activities. The activities in the prevention stage, though closely associated with deterrence and detection, occur after deterrence has failed and before the suspicion or detection of fraud has been accomplished.

Prevention is defined as, "to prevent, to stop or keep from doing or happening, to hinder a person from acting" (Webster, 1997, 1976, & 1941). Prevent is a general term meaning hindering, checking, or stopping. In the fraud arena the use of the term prevention emphasizes both common forms of the definition, to keep from doing and to hinder the fraudster from performing fraudulent

activity. For the purposes of this study the definition of prevention is to hinder, check, or stop a fraudster from performing or perpetrating a fraudulent activity.

Prevention stage activities are intended to prevent the fraud from occurring or to secure the enterprise and its processes against fraud. The ability of prevention to stop losses from occurring versus stopping fraudulent activity from continuing is an important distinction. The latter activities are more appropriately mitigation stage activities. Prevention, when perceived from a security perspective, can be thought of as hardening the target. Prevention actions are frequently similar to security activities in the information technology area. Deploying protective procedures, processes, systems, and verifications, etc. that make fraud harder to commit prevents fraud. Prevention activities are designed to make fraud more difficult to commit. For example, the purpose of the many security features on credit and debit cards is to make card based fraud more difficult. Telecommunications subscription fraud is made more difficult by interactive verification and authentication procedures. Know your customer (KYC) processes for opening accounts in the financial industry make it more difficult for fraudsters to open fraudulent accounts. Querying historical fraud claim files in the insurance hinders fraudsters (Webster, 1997, 1976, & 1941).

Stage Three: Detection

The third stage of the Fraud Management Lifecycle, detection, is characterized by actions and activities intended to identify and locate fraud prior to, during, and subsequent to the completion of the fraudulent activity. While "prior to" may sound like deterrence, it refers to the detection of testing or probing activity used by criminals to facilitate a fraud attempt. To detect is to uncover or reveal, to discover the existence or presence of the fact of something hidden or obscure (Webster, 1997, 1976, & 1941). Detection encompasses three closely related activities in the fraud arena: fraud testing, fraud attempts, and fraud successes.

The separation is derived from the facts that not all fraud attempts are successful and that not all perceived fraud attempts are intended to be successful. These "tests" are attempts to reverse engineer the current fraud policies and detection activities in order to locate vulnerability. Thus, detection in the fraud arena must include revealing the existence of fraud testing and fraud attempts, as well as successful frauds. The identification of testing, attempts, and successes are typically clustered in the detection, prevention, and mitigation stages, but are also relevant in each of the other stages of the Fraud Management Lifecycle. Detection includes identification of a testing component, an attempt component, and a success component. Only detection in all three of these areas provides the required support for the rest of the stages in the lifecycle. To miss any of these is to run the risk of creating a vulnerability that the fraudster will turn to his advantage.

Stage Four: Mitigation

Mitigation is begun once the presence or a reasonable suspicion of fraudulent activity has been detected. In short, mitigation stops fraud. Other common and relevant terms for the activities in this stage are interdiction and intervention. Sometimes mitigation activities are called prevention and aftercare, where the prevention is focused on stopping the ongoing fraud from continuing. Mitigation is defined as, "to cause to become less harsh or hostile" and "to make less severe or painful" (Webster, 1997, 1976, & 1941). Mitigation focuses upon fast actions that are intended to reduce the extent of the fraud, the amount of the associated fraud losses, and the effort and expense required to recover or correct the impact of the fraudulent activity. This last goal is especially important when identity theft and the resulting identity fraud are involved. The faster the fraud activity is detected and mitigation activities initiated, the less time, effort, and expense will have

to be invested in correcting the consumer's credit record. The definition of mitigation in the fraud arena is to stop a fraudster from continuing or completing the fraudulent activity, to reduce their success. Mitigation activities can range from real time to delay. Clearly the faster mitigation activities can be undertaken, the better for all involved, except, of course, the fraudster. The environment in which the business enterprise operates defines the meaning of real time. For example, real time can range from a ten second authorization in the payment card industry to a one minute phone call in the telecommunications industry, to a ten minute instant credit application in the retail industry, to a weeklong mortgage application process, to a month long insurance claim process, to an extended internal employee fraud investigation. Clearly the environment defines the mitigation activities that can be taken in real time.

The fundamental premise is to begin mitigation activities as quickly as possible. The speed with which mitigation can be initiated is constrained by the timeliness and capabilities of the detection systems and processes utilized. If the fraud involves an employee and detection is accomplished through receiving calls from a customer or tips from an external agency, the opportunity to mitigate losses, expenses, and impact will be significantly constrained. If, on the other hand, detection systems can alert special investigations investigators to the strong likelihood of internal fraud before customers and outside agencies become aware of the fraud, the opportunity to mitigate losses, expenses, impact, and exposure will be significantly enhanced. Mitigation performance, then, is constrained by both the business environment and the detection tools being used. Fast mitigation actions provide the promise of speedy termination of the fraud event, reduced losses, and reduced expenses and impact. Much of the resource balancing in the Fraud Management Lifecycle revolves around the appropriate allocation of sufficient, efficient, and early mitigation efforts (Webster, 1997, 1976, & 1941).

Stage Five: Analysis

Analysis is characterized by activities to identify and understand losses that occurred despite the deterrence, detection, prevention, and mitigation stage activities. Analysis must evaluate the impact of fraud management activities upon legitimate customers. The product or service cost structures must be evaluated and understood to ensure the appropriate prioritization of casework. Analysis is defined as, "the separation of anything into its constituent parts or elements, to analyze, to make an analysis of, to study in detail the factors of a situation, problem or the like, in order to determine the solution or outcome" (Webster, 1997, 1976, & 1941).

The analysis stage receives data regarding performance from each of the other stages in the Fraud Management Lifecycle and provides them with feedback regarding performance. Analysis provides the performance reporting metrics that allow fraud management to make informed, calculated, and relevant decisions. Analysis processes include the evaluation of the volume and causes of losses, the evaluation and reporting of analyst and investigator performance, the evaluation and reporting of individual and aggregate rule (detection) performance, the evaluation and reporting on predictive score performance, the individual and aggregate customer service impact for each of the various stages, the analysis of staffing productivity in each of the disciplines, the appropriate mix of resources in each discipline, the performance of new and existing strategies, the comparison of the performance of competing (champion-challenger) strategies, and supporting policy's request for retroactive and prospective hypothetical analysis.

Stage Six: Policy

Policy activities create, evaluate, communicate, and assist in the deployment of fraud policies to reduce the incidence of fraud and the inconvenience to legitimate customers, and to allocate the resources required to successfully combat fraud. Policy is defined as, "wise management, prudence or wisdom in the management of affairs, management based primarily on material interest" (Webster, 1997, 1976, & 1941). Policy must seek to balance deterrent value, loss reduction, sales volume, operational scalability, and cost effectiveness. The ability to balance all of these demands surely requires the wisdom referenced in the definition of policy. In many ways policy development is the process of constantly reassembling the situations just disassembled in the analysis stage. The reassembly needs to take advantage of the knowledge gained by analysis and combine it with internal, external, and interactive environmental factors in order to craft policies that address the whole, while leveraging the knowledge of the parts. Policy development staff is most frequently the leaders within the fraud management organization, as they must be able to consider all the disciplines within the fraud management department, as well as the needs of the rest of the business enterprise.

Stage Seven: Investigation

Investigation activities obtain enough evidence and information to stop fraudulent activity, to obtain recovery of assets or restitution, and to provide information and support for the successful prosecution and conviction of the fraudster(s). Investigation is defined as, "to investigate; a careful search or systematic inquiry; to follow up or make research by patient inquiry, observation, and examination of facts" (Webster, 1997, 1976, 1941). In the fraud arena the definition of investigation needs to be expanded to include the important coordination activities with law enforcement entities.

Fraud investigations are focused upon three primary areas of activity: internal investigations, external investigations, and law enforcement coordination. The first area, internal investigations, includes investigations of employees, contractors, consultants, or vendors. External investigations are conducted on "customers" (fraudulent claims), "fraudsters" (individual crooks), and "organized groups" (an association of criminals). Frequently fraud cases are neither exclusively internal nor external. In these situations, internal fraudsters and external fraudsters work in concert to commit fraud. One of the more common examples of this situation is when a fraudster or organized group targets an employee to assist them with the commission of the fraud. Law enforcement coordination is the provision of information and resources to, and the maintenance of, a partnership with federal, state, regional, and local law enforcement authorities. Rigorous and routine investigations provide for both an incremental lift in deterrence and the maintenance of an effective relationship with law enforcement. A rigorous investigation includes comprehensive and detailed case documentation, complete detailed descriptions of the activity, accurate and complete interview notes, extensive contact information, and high quality physical and digital evidence documentation and storage. Each case is investigated with the idea that it will be prosecuted. Case files are prepared assuming an appeals court level of review. The investigations stage benefits greatly from the planned, systematic search for facts and other supporting information, as well as the ingenuity, initiative, thoroughness, and responsiveness of the investigator. The law enforcement relationship is not a one-way street. An important part of the relationship is providing substantive responses, professional assistance, and detailed documentation when calls and other inquiries are received. Depending on the business environment these requests for information can and are received twenty-four hours a day, 365 days a year. One of the most critical support

components in the investigative function is the development of training on, and maintenance of, detailed investigative procedures (Webster, 1997, 1976, & 1941).

Stage Eight: Prosecution

The communications in this stage are focused upon prosecutorial and judicial authorities as well as with law enforcement. Prosecution is defined as, "the act or process of prosecuting; to conduct legal action against, to pursue by legal proceedings for redress or punishment, especially because of some crime or breach of law" (Webster, 1997, 1976, & 1941). There are three aims of prosecution in the fraud arena. The first is to punish the fraudster in an attempt to prevent further theft. Secondly, prosecution seeks to establish, maintain, and enhance the business enterprise's reputation of deterring fraud, so that the fraud community becomes aware of it. This is accomplished by the aggressive and successful catching and punishing of fraudsters who target the company. The third goal is to obtain recovery or restitution wherever possible. Some would argue that there is a fourth aim, that of satisfaction for punishing the fraudster.

The emotional feelings of satisfaction, though positive, are fleeting and tend to obscure the realistic evaluation of prosecution activities. The importance of prosecution should be limited to deterrence, recovery, and restitution. After a case has been forwarded to law enforcement for the apprehension of a suspect, the philosophical point of no return has been crossed. From this point on, the case should be prosecuted to its natural conclusion. The charges filed should be maintained and the case prosecuted even in the face of offers of restitution and mounting witness expenses. It is always advisable to request appropriate restitution as part of the sentencing recommendations.

An additional activity important to the prosecution stage is the consistent and visible coordination of supportive legislative and regulatory activities to stop fraudulent activity. This activity frequently falls to senior managers and legal counsel due to their experience, industry contacts, and broad perspective. These efforts often require, and should receive, the support of line managers and supervisors in assessing the impact of recommendations, the creation of alternatives, and the creation of committee recommendations and presentations.

2.2 Empirical Review

Hennop, Jefferson and McLean (2001) highlight two main types of cash-in-transit armed robberies. The first type is cross-pavement attacks, these take place outside of the vehicle transporting the money, and the guards/drivers are usual targeted while cash is in transition to the vehicle, the second type of attack is a "heist" in which the vehicle is attacked while moving. The use of illegal firearms or stolen firearms are a certainty, there is a sharp increase in the violence of armed robberies with assault rifles being the preferred weapon of choice. Hennop, Jefferson and McLean (2001) also explain that the Nature of CIT robberies are different and unique from hijackings and bank robberies; continues that the following features as typical of a CIT robbery, Low level of concealment, force is displayed overtly, little attempt to minimize public witnesses, and rifles are used to hand guns (preference for greater firepower) .

Research in Greater Manchester in 2003 revealed that one quarter of "street crimes", such as cash in transit robbery and bag snatching were related to ATMs. The study included an intervention in which a small "personal space zone" was painted on the ground around selected machines. In a six month period, robbery around the experimental sites declined from an average of 27 down to 9.2 per site (Holt & Spencer, 2005). According to research done by Smith and Louis (2010), United Kingdom (UK) has considerable risks in CIT robberies. In 2005 the UK had a total number of 763

reported cases of CIT robberies. In comparison with South Africa, the study found out that South Africa had 509 cases of CIT theft cases the same year. According to the Brazilian Federation of Bank, in 2009 the country lost $30 Million due to bank robberies and Cash-in-transit robberies (Smith, 2010). Febraban stated that money stolen in a CIT robbery rarely exceed $300 000.00 but in some cases like an incident that happened on the 5th of November 2009 where a total of $4 Million was stolen (Smith, 2010). In Brazil 10% of all bank robberies are directed at armored vehicles and cash in transit (Smith, 2010).

Ikpefan (2007) examined money transfer services in banks through the Western Union Money Transfer. The dynamism in business environment made it imperative for banks to adopt an anticipating stance towards changes. The study investigated and tested the loss of money in transit by comparing traditional and western union money transfer using interviews and questionnaires. The chi square statistic was used to test the result. The study revealed that western union money transfer had really reduced the frequency of loss of money in transit in Nigeria. Due to customers complains, the study recommended that bank management should come out with a very clear policy statement concerning exchange rate.

Gill (2001) conducted a study in Australia employing research from the Australian Institute of Criminology's National Armed Robbery Monitoring Program and examined CIT armed robberies, the offenders who commit them and their perceived level of professionalism. The study involved 341 robbers, found out that offenders who committed armed robberies on CIT operators were the most informed when it came to analyzing and reviewing the risks associated with the robbery The study also considered the nature of CIT attacks overseas and the types of crime prevention strategies used in those countries. The results of the study also indicated that CIT-type armed robberies are generally considered to be the work of professional armed robbers and there is anecdotal evidence of a recent rise in these types of incidents. The study also stated that successful armed robbers are those who take risks; however, there is little research into how those risks are managed.

Expansion was done on Gill's work by Pillay (2008) who confirmed that CIT offenders gathered intelligence on their targets and spent time researching the movement of cash deliveries/collections and would select their targets according to the perceived risks. The primary target selection criteria will be targets perceived as 'soft' with medium to high reward. Indicators of 'soft' targets include companies using transportation equipment not fit for the job and unarmed CIT operators. Smith and Louis (2010) stated that the major industry participants, mostly commercial banks, have invested heavily in improving the safety of their employees. Some of the improvements are better overall design of armored vehicles to enhance crew safety including the installation of GPS monitoring on all vehicles, the installation of single person entry technology on all vehicles; implementation of vehicle CCTV systems; and improved external vehicle lighting, a full review of armored vehicle operator recruitment and induction training and the implementation of advanced annual armed robbery scenario training.

In the Kenyan context, Fayo (2015) states that G4S Security Company was involved in cash in Transit theft of cooperative bank of Kenya cash which was being transported from the bank's Maua branch in Meru to its Koinange branch in Nairobi.Ksh.80 million was stolen in the process. The company has also been involved in other cases of theft with consolidated bank of Kenya. It had previously been ordered to pay Ksh.18.55 Million to consolidated bank for being involved in cash in transit theft. Cash in transit theft is not only done by the G4S security company but also

other security companies contracted to transport cash (Ndonga, 2014). A recent case was KK security officers making away with a total of KSh.82 million which they were transporting from Westlands to the Central Bank of Kenya. Despite the fact that the distance between Westlands and Central bank of Kenya was short, money was still being stolen. Poor cash transportation is to blame for that.

According to Middle East & North Africa Financial Action Task Force (2015), physical transportation of cash as a method of money laundering was not restricted to a particular type of crime. The methods used to physically transport criminal cash were dependent on a decision making process undertaken by the criminal. It was apparent from the questionnaire responses that this phenomenon of legitimate cross-border cash transportation was not well understood generally. The responses showed that most countries were aware that air passengers and persons in cars carry cash legitimately across borders. However, substantially fewer had any experience of cash moving in cargo and mail for legitimate purposes, and yet huge amounts of cash (the equivalent of tens, and sometimes hundreds of millions of US dollars in a single shipment) are transported between major financial institutions by air cargo every day, shipments that are generally subject to very little scrutiny by customs authorities. This general lack of knowledge and/or understanding is significant. Without a thorough understanding of the methods and techniques of legitimate cross border cash transportation, the customs procedures and documentation applicable and the mechanisms that drive these methods and techniques, it could be very difficult for the authorities in a country to be able to tell if a shipment of cash was legitimate or not. Moreover, without this understanding, countries would not be able to assess whether their legislative processes were sufficient to allow their customs and border authorities to control cross-border cash transportation effectively.

CIT armed robberies generally involved planning by multiple offenders, armed with firearms, who are seeking substantial gains. In line with this profile, it was likely that most CIT offenders will be professional armed robbers. This is supported by Gill (2001) in one of the few studies undertaken in this area. Gill (2001) studied 341 robbers who targeted a variety of locations and noted that a consistent pattern emerged; CIT robbers were the most organized and made the most effort to manage possible risks. Other studies have also noted that CIT offenders collected information and gather intelligence about companies they want to target and that they also researched when and where movement of cash takes place (Pillay 2008).

Hepenstal and Johnson (2010) investigated the concentration of cash-in-transit robbery. According to the study, no systematic studies of the spatial distribution of CIT robbery existed and therefore the authors sought to fill this gap using data for London, UK. In the first instance patterns were analysed for the whole of the city. To provide more detailed analysis, a case study was conducted in one area identified as a hotspot. In that area, a survey was conducted to identify the actual distribution of potential CIT targets as well as the offence locations. The possible influence of the configuration of the street network was also examined. The findings suggested that CIT robbery clusters in space more than would be expected on the basis of the distribution of targets, and that the risk of CIT robbery was particularly acute around major intersections.

3.0 RESEARCH METHODOLOGY

The study adopted a descriptive survey design. The target population for the study was 43 licensed and operational commercial banks in Kenya. The sampling frame of the survey of the banks was

one head of operations and head of finance from each of the 43 commercial banks located in Nairobi County. A multi stage sampling approach was used. In the first stage, a census of all the 43 commercial banks was conducted, that is, the units of analysis were the commercial bank. In the second stage, purposive sampling was used where two respondents from every organization were taken. In particular the head of operations and the head of finance were sampled for the study. Primary data on cash reconciliation was collected using questionnaires. Secondary data on cash reconciliation (Frequency of reconciling various accounts), Return on equity and return on assets were obtained using attached secondary data sheet. SPSS was used to produce frequencies, descriptive and inferential statistics were used to derive conclusions and generalizations regarding the population. The particular descriptive statistics were frequencies, mean scores and standard deviation. The particular inferential statistic was regression and correlation analysis. The analysis of variance (ANOVA) was checked to reveal the overall model significance. A critical p value of 0.05 was used to determine whether the overall model was significant or not. The individual regression coefficient was checked to see whether the independent variable cash reconciliation significantly affected the financial performance. A critical p value of 0.05 was used to determine whether the individual variable was significant or not.

A regression model was used to link the independent variable to the dependent variable as follows;

$Y = \beta_0 + \beta_1 X + \mu$

Where;

Y = Financial Performance

X_1 = Cash Transport

μ = Error Term

The specific models were as follows;

$ROA = \beta_0 + \beta_1$ Cash Transport$+ \mu$

In the model, β_0 = the constant term while the coefficient $\beta_i i = 1$ were used to measure the sensitivity of the dependent variable (Y) to unit change in the predictor variables X. μ is the error term which captures the unexplained variations in the model (Olusola et. al, 2013).

4.0 RESEARCH FINDINGS AND DISCUSSIONS

4.1 Response Rate

A total of 86 questionnaires were administered out of which 60 of them were properly filled and returned representing an overall successful response rate of 69.8%

4.2 Attributes of Cash Transport

The objective of the study was to assess the effect of cash transport on the financial performance of commercial banks in Kenya. The respondents were asked to respond to some statements on cash transport based on a scale of 1 to 5 where 1 represented strongly disagree and 5 represented strongly agree. The results are given in Table 1. The study findings revealed that all of the respondents agreed that the bank had a cash transport policy and that the bank regularly reviewed the contracts of companies which transported its cash. 90% of the respondents agreed that the bank had tracking devices in the vehicles that transported its cash while all the respondents agreed that the bank engaged administrative police in security arrangements when transporting cash. Those

respondents who agreed that the bank had invested in a chase car which was used when transporting cash were 80%. The mean response of 4.52 implied that the respondents agreed on most statements regarding cash transport. The standard deviation of 0.67 showed that there was a small variation in the responses given by the respondents.

Table 1: Attributes of Cash Transport

	1	2	3	4	5	Mean	Std Dev
The bank has a cash transport policy	0.00%	0.00%	0.00%	30.00%	70.00%	4.70	0.46
The bank regularly reviews the contracts of companies which transport cash for them.	0.00%	0.00%	0.00%	40.00%	60.00%	4.60	0.49
The bank has tracking devices in the vehicles that transport cash	0.00%	10.00%	0.00%	30.00%	60.00%	4.40	0.92
The bank engages Administrative police in security arrangements when transporting cash	0.00%	0.00%	0.00%	30.00%	70.00%	4.70	0.46
The bank has invested in a chase car which is used when transporting cash	0.00%	10.00%	10.00%	30.00%	50.00%	4.20	0.99
Average						**4.52**	**0.67**

4.3 Relationship between Cash Transport and Return on Assets

The study sought to establish the relationship between cash transport and Return on Assets. An ordinary least square regression model was used. The results of the model summary are given in Table 2. The findings revealed that cash transport explained 11.5% of the changes in ROA of commercial banks operating in Kenya in the study period while 88.5% of the changes in ROA of the commercial banks was explained by other factors other than cash transport that were not included in the model.

Table 2: Relationship between Cash Transport and ROA (Model Summary)

R	R Square	Adjusted R Square	Std. Error of the Estimate
.339	0.115	0.1	107.8743

Furthermore the model fitness was assessed by comparing the F critical and F calculated. The results for F-calculated are as presented in Table 4.12. The F-Critical, $F_{0.05, 1, 58}$ was 1.35. Since F calculated, 7.521, was greater than F-Critical, $F_{0.05, 1, 58}$, 1.35, the study concluded that the model was satisfactory. This is further supported by a p-value of 0.008 which was less than the critical value also known as the probability value (p) which was statistically set at 0.05.

Table 3: Relationship between Cash Transport and ROA (Model Fitness)

	Sum of Squares	Df	Mean Square	F	Sig.
Regression	87519.36	1	87519.36	7.521	0.008

Residual	674938.4	58	11636.87
Total	762457.7	59	

The results in Table 4 further presented coefficients of the regression model. These showed that the relationship between cash transport and ROA was positive and significant. This was supported by a beta coefficient of 1.087 and P-Value of 0.008. The findings implied that an improvement in cash transport practices led to an improvement in ROA.

Table 4: Relationship between Cash Transport and ROA (Model Coefficients)

	B	Std. Error	t	Sig.
(Constant)	-1.457	8.480	-1.718	0.091
Cash Transport	1.087	3.969	2.742	0.008

Model

ROA= -1.457 + 1.087 Cash Transport

The study sought to test the null hypothesis below.

H_0: Cash Transport does not affect the financial performance of commercial banks in Kenya.

The results of the regression model between cash transport and ROA were used to test the null hypothesis. The rejection criterion was based on the P-value of the regression model. A p-value less than 5% level of significance led to rejection of the null hypothesis while a p-value greater than 5% level of significance led to failure in rejection of the null hypothesis. Based on the findings, the study rejected the null hypothesis that cash transport did not affect the financial performance of commercial banks in Kenya. This is because the probability value (p-value = 0.008) was less than the critical value of 0.05 hence the study concluded that cash transport affected financial performance of commercial banks in Kenya.

5.0 SUMMARY OF FINDINGS, CONCLUSION AND RECOMMENDATIONS

5.1 Summary of Findings

The objective of the study was to assess the effect of cash transport on the financial performance of commercial banks in Kenya. The study findings suggested that all the respondents agreed that the bank had a cash transport policy and that the bank regularly reviewed the contracts of companies which transported their cash. 90% of the respondents agreed that the bank had tracking devices in the vehicles that transported cash while all respondents agreed that the bank engaged in administrative police in security arrangements when transporting cash. Those respondents who stated that their bank had invested in a chase car which was used when transporting cash were 80%. The mean response of 4.52 indicated that the respondents agreed on most statements regarding cash transport. The standard deviation of 0.67 implied that there was a small variation in the responses given by the respondents.

Further findings showed that cash transport explained 11.5% of the changes in ROA of commercial banks operating in Kenya. Furthermore, the association between cash transport and financial performance was found to be positive. The regression results revealed that the relationship between cash transport and ROA was positive and significant implying that an improvement in cash transport practices led to an improvement in financial performance of commercial banks.

The study findings supported the argument by Bold (2011) and Bean (2009) that banks should put

in place security measures like integrant guidance on response programs for unauthorized access to customer information and customer notice, access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals; access restrictions at physical locations containing customer information, encryption of electronic customer information and cash including while in transit or in storage so as to reduce fraud related to cash in transit and cash in storage. The study findings also concurred with the findings of a study by Gill (2001) which showed that proper prevention mechanisms of robberies of cash in transit reduced banks' lose hence boosting trust and performance.

The findings also endorsed the argument by Smith and Louis (2010) that in order to reduce cash in transit theft, some of the measures to be taken was investing heavily in the overall design of armored vehicles to enhance crew safety including the installation of GPS monitoring on all vehicles, the installation of single person entry technology on all vehicles; implementation of vehicle CCTV systems; and improved external vehicle lighting, a full review of armored vehicle operator recruitment and induction training and the implementation of advanced annual armed robbery scenario training.

5.2 Conclusion

Based on the study findings, the study concluded that cash transport explained 11.5% of the changes in ROA. Furthermore, the association between cash transport and financial performance was positive. The study also concluded that the relationship between cash transport and ROA was positive and significant implying an improvement in cash transport practices led to an improvement in ROA.

5.3 Recommendations

The study recommends that commercial banks and other financial institutions involved in handling of cash should The commercial banks should have a cash transport policy which clearly stipulates how cash in transit should be handled, regularly review the contracts of companies which transport cash for them so as to avoid known routines, have tracking devices in the vehicles that transport cash, engage administrative police in security arrangements when transporting cash and invest in cash in transit measures like chase cars.

REFERENCES

Archer, M., & Tritter, J. (2000). *Rational choice theory: Resisting colonization.* New York: Routledge.

Beranek W (2000). *Analysis for financial decisions,* (15thed.), Irwin, Homewood.

Clarke, R. V., & Felson, M., (2008). Introduction: Criminology, routine activity, and rational choice. In: R. V. Clarke & M. Felson, eds. *Routine Activity and Rational Choice*.1st ed. New Jersey: Transaction, pp. 1 - 14.

De Haan, W., & Vos, J. (2003). A crying shame: The over-rationalized conception of man in the rational choice perspective. *Theoretical Criminology, 7*(1), p. 29 –54

Erkki, K. (2004). Cash management behavior of firms and its structural change in an emerging money market. Faculty of Economics and Business Administration, Department of Accounting and Finance, University of Oulu

Fayo, G. *(2015). Co-op Bank sues security firm G4S over 2010 robbery. Retrieved from (www.businessdailyafrica.com).*

Gill, M. (2001). The craft of robbers of cash-in-transit vans: crime facilitators and the entrepreneurial approach. *International journal of the sociology of law*, *29*(3), 277-291.

Grossman, R. (2010). *Unsettled account: The evolution of banking in the industrialized world since 1800*. Princeton University Press. p. 96.

Hennop, E., Jefferson, C., & McLean, A. E. (2001). *The challenge to control: South Africa's borders and borderline* (No. 57). Institute for Security Studies.

Hepenstal, S., & Johnson, S. D. (2010). The concentration of cash-in-transit robbery. *Crime Prevention & Community Safety*, *12*(4), 263-282.

Ikpefan, O. A. (2007). Money transfer services in banks: A case study of Western Union Money Transfer. *Nigerian Journal of Banking and Financial Issues*, 122-140.

Mbuguah, C. (2013). *Response strategies to fraud by the listed commercial banks in Kenya.* (Unpublished MBA Project, University of Nairobi).

Myers, N. (2010). *Review of the roots of youth violence: Literature reviews*: Volume 5, Chapter 3.

Ndonga, S. (2014). Police recovers Sh13m stolen cash-in-transit. Retrieved from (www.capitalfm.co.ke)

Njiraini, J. (2010). *G4S unveils tough measures to prevent theft of transit cash.* Retrieved from (www.standardmedia.co.ke)

Nwankwo, G. O. (1992). *Banking frau*d. Lecture delivered at the 5th Anniversary of Money market Association of Nigeria.

Pandey, S., & Jaiswal, V. K. (2011). Effectiveness on profitability: working capital management. *SCMS Journal of Indian Management*, *8*(1), 73.

Pillay K. (2008). The impact of stress and trauma on the occupational environment of CIT security officers—an exploratory perspective. *International Society for Criminology XV World Congress, Barcelona 20–25 July 2008*

Poisat, P., Mey, M., & Theron, A. (2014). Social support key to cash in transit guards' psychological wellbeing. *Problems and Perspectives in Management*, *12*(4), 312-319.

Smith, L., & Louis, E. (2010). Cash in transit armed robbery in Australia. *Trends and issues in crime and criminal justice*, (397), 1.

Taylor, J. (2007). Company fraud in Victorian Britain: The Royal British Bank Scandal of 1856. *The English Historical Review*, *122*(497), 700-724.

Tremblay, P. (2008). Searching for suitable Co-Offenders. In: R. V. Clarke & M. Felson, eds. *Routine Activity and Rational Choice*. New Jersey: Transaction, pp. 17 – 36

Van Anholt, R. G. (2014). Optimizing logistics processes in cash supply chains. Retrieved from: http://asia.iccos.com/files/Dissertation_Roel_G_van_Anholt.pdf