EFFECTIVENESS OF FRAUD RESPONSE STRATEGIES ADOPTED BY CO-OPERATIVE BANK OF KENYA LIMITED

TIMOTHY SISA WANYAMA

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE DEGREE OF MASTER OF BUSINESS ADMINISTRATION (MBA) SCHOOL OF BUSINESS, UNIVERSITY OF NAIROBI.

OCTOBER 2012

DECLARATION

I declare that this is my original work and has not been submitted for examination in any other university or College for Examination or Academic purposes.

Signature _____ Date _____

Timothy Sisa Wanyama

D61/70791/2008

This research project has been submitted for examination with my approval as the university supervisor.

Signature _____ Date _____

Professor: Martin Ogutu

Department of Business Administration

School of Business

University of Nairobi

DEDICATION

This strategic management paper is dedicated to God for having given me the grace of life and strength, my wife Jacinta Nasimiyu and our lovely daughter Audrey Nafula who were both supportive during the entire period of study.

Special dedication goes to my Grandmother Agnes Navangala who despite having never gone to any formal school kept encouraging me to study to the highest level possible. I am proud of her. To my Parents Mr. and Mrs. Japhew Wanyama, thanks you so much for your commitment to ensure every member of your family gets formal Education.

ACKNOWLEDGEMENT

I thank almighty God for the grace of life and for being my shepherd during the long period of writing this final paper.

I highly appreciate the extensive help and support both morally and financially from my friends, colleague's and workmates during the entire period of my study.

I do acknowledge the work, time and academic support from my supervisor whose input was critical in writing and refining my final project paper.

My appreciation goes to my wife Nasimiyu for all the overwhelming support and encouragement she gave me, my siblings, my parents Japhew Wanyama and Jeritah Nashevanda not forgetting a loving Grand Mother, Agnes Navangala who have been a source of motivation, support and encouragement during the entire course of my project.

ABSTRACT

Fraud is among the greatest challenge facing organization today, If not well managed; it may lead to their downfall. Fraud in banking sector has been attributed to advancement in technology and weak internal controls. The objectives of this study were to identify the types of fraud, response strategies and the effectiveness of the response strategies to fraud at Co-operative bank of Kenya. Previous studies on this topic of fraud established that strict internal controls assist to detect, prevent and control fraud in institution. Various strategies such as risk monitoring, Internal audit and staff screening, are currently being used to manage fraud. At the time of the study, no local or international studies had ever been done on effectiveness of response strategies to fraud adopted by commercial banks in Kenya, thus there was a need to carry out this study. This was a case study aimed at getting detailed information regarding effectiveness of responses strategies to fraud at Co-operative bank of Kenya. The primary data was collected using an interview guide. The interview guide contained open-ended question that enabled the researcher to collect in-depth qualitative data. The interview data was examined for completeness and consistency after which it was analyzed using the content analysis method. The information was presented in a continuous prose. The researcher interviewed all the six proposed managers making a response rate of 100%. The study concludes that ineffective strategies cannot adequately control fraud, managing the risk of fraud will ensure growth, customer confidence and security for the bank. The study recommends that commercial banks must examine each response strategy for effectiveness and develop, modify or discard those that are not effective. The study also recommends reforms in the police and judiciary, enhancement of security features on key identification documents, staff motivation and whistle blowing.

TABLE OF CONTENTS

DECLARATION ..... **ii**
DEDICATION ..... **iii**
ACKNOWLEDGEMENT ..... **iv**
ABSTRACT ..... **v**
CHAPTER ONE:INTRODUCTION **1**
1.1 Background of the study 1
1.1.1 Response strategies 1
1.1.2 Fraud and related challenges 3
1.1.3 Banking Industry in Kenya 4
1.1.4 Co-operative bank of Kenya Limited 6
1.2 Research Problem 7
1.3 Research Objectives 8
1.4 Value of the Study 9
CHAPTER TWO:LITERATURE REVIEW **10**
2.1 Concept of strategy 10
2.2 Organization and Environment 11
2.3 Response strategies 13
2.4 Concept of fraud and related challenges 17
CHAPTER THREE:RESEARCH METHODOLOGY **20**
3.1 Introduction 20
3.2 Research Design 20
3.3 Data Collection method 21
3.4 Data Analysis 21
CHAPTER FOUR:DATA ANALYSIS,FINDINGS AND DISCUSSION **22**
4.1 Introduction 22
4.2 Types of Fraud 22
4.3 Response strategies to fraud 24
4.4 Effectiveness of fraud response strategies 28
4.5 Discussions of Findings 31

CHAPTER FIVE:SUMMARY, CONCLUSION AND RECOMMENDATIONS 38
5.1 Introduction 38
5.2 Summary of findings 38
5.3 Conclusions of the Study.....41
5.4 Limitations of the Study 42
5.5 Suggestions for further research.....42
5.6 Recommendations for policy and practice 43

REFERENCES 44
APPENDICES.....47
Appendix I: Cover Letter.....47
Appendix II: Interview Guide 48
Interview Questions.....48

CHAPTER ONE
INTRODUCTION

1.1 Background of the study

Fraud is an intentional misrepresentation, concealment or omission of the truth or material facts for the purpose of deception or manipulation resulting to injury of a person or organization (Fitch, 1997). Bank fraud refers to all forms of frauds committed against banks from internal or external sources (wells, 2007). The effects of frauds are seen in downfall of organization as a result massive loss of revenue, tainted public reputation and image (Norton, 1994). Frauds comes in various forms, sizes, shapes and fashions which include identity theft, accounting fraud, Fraudulent loans, ATM theft, cybercrime, skimming, false valuations, accounting fraud, check fraud and mail fraud (Wells, 2007).

The banking sector thus faces a never-ending task in seeking ways to stay one step ahead of the fraudsters in preventing fraud, It is therefore important that they get their response strategies right, if they don't, they may not survive to get it right the next time. The banking sector is a critical component of any economy and therefore crafting effective fraud response strategies should be a top most priority for the management.

1.1.1 Response strategies

Response strategies are a set of decisions and actions that assist organizations achieve set objectives, they entail formalization and implementations of strategic plans (Pearce and Robinson, 2011). Response strategies help organizations in assessing their current position, where they want to go and how to get there. Wanjiru (2011)

noted three components of an organization strategy that are critical in identifying response strategies to environmental challenges, they are setting objectives and goals, outlining strategic direction for business activities and adopting a competitive strategy.

Response strategies adopted by organizations are either operational or strategic in nature. In the study by Hunger and wheelen (1990), operational responses are applied in areas such as marketing, finance, human resource and Research and development. In the study by Wanemba (2010), operational responses are concerned with efficiency of operations in an organization. They are usually crafted by organizations to assist in maximizing utilization of existing resources with the aim of developing distinctive competence that give a competitive edge.

Strategic responses are crafted at corporate and business level of an organization to address long term environmental challenges; their implementation requires participation of the entire members of the organization. Development and implementation of strategic response entails rational analysis, intuition, experience, resources, right climate, competence and capacity to respond by the organization (Ansoff, 1988; Pearce and Robinson, 2011).

Strategic response may also be proactive or reactive, proactive strategies are crafted from existing strategic actions and approaches that are still viable, reactive strategies are developed as a response to unexpected change in business environment (Thompson, Strickland, Gamble & Jaine, 2006). Some of the response strategies to fraud include, sharing knowledge in fraud forums, setting up fraud management units, detection and prevention techniques, establishing fraud policy, strict regulations,

legislation of laws on bank fraud, establishing code of conduct for employees, Risk assessments and Management review.

1.1.2 Fraud and related challenges

Fraud includes activities such as theft, corruption, conspiracy, embezzlement, money laundering, bribery and extortion. It is an intentional misrepresentation, concealment or omission of the truth or material facts for the purpose of deception or manipulation resulting to injury of a person or organization (Fitch, 1997). The effect of frauds can be seen in the downfall of entire organizations, massive investment losses, significant legal costs, incarceration of key individuals, and erosion of confidence in capital markets of countries, damage to reputations, brands, and images of many organizations around the globe.

Fraud cuts across all sectors of the economy, within and outside borders of a nation with the banking sector top of the most affected. The major types of fraud are Asset misappropriation, accounting fraud, bribery and corruption fraud, cybercrime, money laundering, tax fraud, illegal insider trading and sustainability fraud (PWC Global Economic crime survey, 2011).

Fraud occurs when a number of factors are in place, for instance pressure to meet goals, need for personal gain, motivation to commit fraud, existence of opportunity, week internal controls, poor organization culture and greed (Wells, 2007, KPMG Singapore fraud survey, 2011; HM Treasury advisory report, 2003). When fraud is discovered organization deal with it in different ways such as firing the employees involved, transferring staff, civil action, informing police, doing nothing, warning staff, reporting to relevant regulatory authorities (PWC Global Economic Crime Survey, 2011; KPMG Fraud and Misconduct Survey, 2010).

The fight against fraud faces a number of challenges a cross all sectors, this are dilemma of reporting fraud, poor organization perception of fraud, lack of goodwill from top management in the fight against fraud, poorly established and equipped Judicial systems, lack of adequate technology, perceived damage to public image and reputation (Norton, 1994; PWC Risk Survey, 2011).

1.1.3 Banking Industry in Kenya

The Companies Act (Cap 286), the Banking Act, the Central Bank of Kenya Act and the various prudential guidelines issued by the Central Bank of Kenya (CBK), governs the Banking industry in Kenya. The banking sector was liberalized in 1995 and exchange controls lifted. The CBK, which falls under the Minister for Finance's docket, is responsible for formulating and implementing monetary policy and fostering the liquidity, solvency and proper functioning of the financial system. CBK also acts as a banker, agent and advisor to the government of Kenya.

The financial sector in Kenya comprises of commercial banks, non-bank financial institutions (NBFIs), development finance institutions, insurance companies and stock exchange. As at 30th June 2011, the sector comprised of forty three commercial banks, one mortgage finance company, six deposit taking microfinance institutions, two credit reference bureaus, three representative offices of foreign banks and 124 foreign exchange bureaus. A few large banks most of which are foreign-owned, though some are locally owned, dominate the banking industry. Seven of the major banks are listed on the Nairobi Stock Exchange. The banks in Kenya have formed an umbrella body called Kenya Bankers Association (KBA) which champions and addresses issues affecting member banks. The commercial banks and non-banking institutions offer corporate, investment and retail banking services. Brownbridge & Harvey (1998)

noted that since independence expansion and diversification of the financial system in terms of numbers and range of financial institutions have accompanied the growth of Kenyan economy.

The banking industry in Kenya faces challenges such as fraud, changes in the regulatory framework, declining interest margins due to customer pressure, increased demand for non-traditional services including the automation of a large number of services, increased competition from microfinance institutions, introduction of non-traditional players, who now offer financial services and products for instance mobile companies such as Safaricom (Brownbridge & Harvey, 1998; African Banker, 2011).

Bank fraud refers to all kinds of intentional, dishonest and non violent acts committed against banks by insiders, consumers, businesses and other financial institutions to secure unlawful or unfair gain whether in cash or in kind (Norton, 1994; Wells, 2007). Financial activities have been in existence since 2000.B.C when goldsmith kept jewelers and other valuable items for rich merchants (Jhingan & Jinhgan, 1994). According to Neil ford (African banker 1st quarter, 2011), the financial crime has existed as long as there has been financial activity.

Bank frauds commonly occur in new accounts than established ones where they are opened with false identifications, using checks stolen from legitimate business, or where an individual opens a personal account with checks in other people's names (Wells, 2007). Bank fraud comes in various shapes, sizes, complexity and fashions and each of them continue to flourish till the authorities and public are made aware of their existence and adequate counter measures taken. According to Norton (1994), banks are to blame for the increase in fraudulent activity because they commit contributory negligence by embracing technology to provide better services to

customers and failing to develop systems to protect the integrity of these creative technologies.

Bank fraud can be curbed through detection and prevention methods (Norton, 1994; ACFE report 2010). Mike stinger of Us Secret Service emphasized the need of awareness by noting that if you have never seen it before, you can't have systems designed to identify it. The major types of fraud affecting banks are Asset misappropriation, accounting fraud, bribery and corruption, cybercrime, money laundering, tax fraud, illegal insider trading and sustainability fraud, identity theft, ATM fraud, Mobile Banking fraud, System fraud, staff fraud, Account take over and bank robbery (PWC Global Economic crime survey, 2011).

1.1.4 Co-operative bank of Kenya Limited

The Co-operative Bank of Kenya Limited ('the Bank') is incorporated in Kenya under the Company's Act (cap 486), and licensed to do the business of banking under the Banking Act. The Bank was initially registered under the Co-operative Societies Act (cap 460) at the point of founding in 1965 and later in 2008 it was incorporated under the Companies Act. The Bank was listed on NSE on 22 December 2008 with Coop Holdings Co-operative Society Limited having a majority share with a 64.56% stake. The Bank runs four subsidiary companies, namely: Co-op Trust Investment Services Limited, Co-operative Consultancy Services (K) Limited, merchant and investment banking subsidiary and the Kingdom securities Limited.

The bank On August 7th, 1997 suffered a major setback from a terrorist bombing that completely destroyed the Bank's Head office, Co-operative House. The impact of the attack was felt in the subsequent years where the bank reported losses till the year 2000.Since then, the bank has maintained a sustainable growth in profitability despite

the harsh economic environment. The number of branches, ATMs, customers, employees, Dividends and earnings per share and Capital has grown tremendously. The bank plans to open several branches in the East African region. The bank has suffered losses resulting from fraud committed from both internal and external sources and consequently has put in place several response measures to contain and eventually stop all forms of fraud. Some of the measures include a closer monitoring of all account activities, control for all access points and installing cameras in all its ATM lobbies.

1.2 Research Problem

Strategies provide an overview of the direction an organization intends to take in the short term and long term period. Strategies are executable plan of actions that enable organizations respond to internal and external challenges and describe how they will achieve their goals (Johnson and Scholes, 2002; Thompson et al, 2006). Organizations often formulate company, product and service strategies to drive operational, support and managerial processes. When an organization is affected by fraud, the initial actions taken in the first few hours, days and weeks assist in limiting the impact of fraud. Organizations with effective response strategies to fraud are likely to reduce impact of fraud by preventing further lose, recovering any losses incurred, pursuing criminal action where necessary and safeguarding their reputation (HM Treasury advisory report, 2003; Wanemba, 2010).

Employees, customers and business organizations have committed various frauds against Co-operative bank of Kenya. Employee frauds have taken the form of stealing cash directly from tills or intentionally crediting their accounts with customer funds. The customers and business organization commit frauds by colluding with employees

who furnish them with clients data and the weak internal controls. Despite the several measures put in place such as security camera's, access control, detection system, accounts monitoring systems, Compliance units and staff code of conduct, fraud cases are is still being reported.

There are previous studies done by scholars on this topic of fraud and response strategies such as, Mbwayo (2005) did a study on strategies applied by commercial banks in anti-money Laundering compliance programs, Njagi (2009) looked at effectiveness of know your customer policies adopted by commercial banks in Kenya in reducing money laundering and fraud incidences, Cheptumo (2010) studied response strategies to fraud related challenges by Barclays Bank of Kenya, Wanemba (2010) conducted a study on strategies applied by commercial banks in Kenya to combat fraud and Wanjiru (2011) studied strategic responses of Equity Bank to fraud related risks. None of the above reviewed studies focused on effectiveness of fraud response strategies adopted by Co-operative bank of Kenya. This study aims to fill the knowledge gap by establishing the effectiveness of fraud response strategies adopted by Co-operative bank of Kenya. The study seeks to answer the questions: what are the response strategies adopted by Co-operative bank of Kenya in dealing with fraud and how effective are they?

1.3 Research Objectives

The study will aim to achieve the following objectives,

i. To determine the types of frauds encountered by Co-operative Bank of Kenya Limited.
ii. To establish the response strategies adopted by co-operative bank of Kenya Limited in dealing with fraud.

iii. To determine effectiveness of fraud response strategies adopted by co-operative bank of Kenya Limited.

1.4 Value of the Study

The students and academicians will use this study as a basis for discussions and further research on topic of fraud, response strategies to fraud and effectiveness of response strategies to fraud. The study will also be a source of reference material for future research on related topics. The study will seek to fill the knowledge gap left out by past studies on effectiveness of response strategies to fraud related activities. The study will also highlight important relationships that require further research in the area of response strategies to fraud.

The bank managers at Co-operative Bank of Kenya will be enlightened regarding strategic responses to fraud related activities and how their understanding can help reduce or curb fraud related activities encountered in their operations. They will be able to ascertain those strategies that are effective and warrant continuation and those that require modifying or discarding.

The study will also help other managers in the banking sector to know the various fraud response strategies in the market and how they can be applied in their operations. They will also learn various methods used in gathering and applying strategic responses which would help them improve their management styles. Since fraud is universal, they will be able to learn and adopt some strategies applied in other regions to curb fraud thereby minimizing fraud occurrences in their organizations.

CHAPTER TWO
LITERATURE REVIEW

2.1 Concept of strategy

Ansoff and MacDonnell (1990) defined strategy as a set of decision-making rules that guides organization behavior. They noted that the process of strategy formulation sets the general direction in which the firm's position will grow and develop. Thompson et al (2006) defined strategy as a management's game plan for growing business, staking out a market position, attracting and pleasing customers, competing successfully, conducting operations and achieving objectives. A strategy thus is simply an executable plan of action that describes how an organization intents to achieve set goals and objectives (Pearce and Robinson, 2011).

Environmental turbulence makes existing strategies obsolete. In order for organization to succeed in such conditions, they have to develop new strategies whose aggressiveness match the environmental turbulence, furthermore Strategy is a very powerful tool for coping with conditions of change which surround organizations today (Ansoff & MacDonnell, 1990). Crafting strategies is important for any business organization that wants to survive. Effective formulation and implementation of strategies that drive operational, support and managerial processes helps to deal with environmental turbulence. According to Thompson et al (2006), response strategies are either proactive or reactive, reactive strategies are developed as a response to environmental turbulence.

Strategy development involves rational analysis, intuition, experience, and emotion. Rational analysis helps management to have a basis for comparing and evaluating alternatives, understanding issues by providing guiding questions and framework for

organizing the information gathered. Successful strategies have simple goals, are consistent, are long-term in nature, are designed after a careful scanning of the environment and lastly they are effective in exploiting internal strength while protecting the areas of weakness (Grant, 1998 and Thompson et al, 2006).

2.2 Organization and Environment

The environment consists of external and internal aspects of the firm which a strategist needs to understand, monitor and position the organization to manage the opportunities and threats thereof (Grant, 1998; Johnson and Scholes, 2002). These aspects relates to economy, technology, demographics, social and government. Pearce and Robinson (2011) defined a business environment as all those factors beyond the control of the firm that influence its choice of direction, action, organization structure and internal process. The impact of environment on an organization is thus wide and varied and therefore requires proper planning.

Environment can be relatively stable or highly turbulent. Each level of environmental turbulence has different unique characteristics and requires different strategies and firm capabilities (Ansoff and MacDonnell, 1990; Johnson and Scholes, 2002). Strategic Management relates to positioning and relating a firm to its environment in a way that will assure continued success. This requires application of various principles, techniques and advanced tools in strategic management. Understanding the environment is therefore critical to the firm's success. An analysis of key variables such as politics, economy, social, technology, ethics and legal factors are using PESTEL and SWOT analysis techniques are desirable in understanding the environment (Johnson and Scholes, 2002; Pearce and Robinson, 2011). According to Grant (1998), the prerequisite for effective environment analysis is identifying the

core elements of a firm's business environment, which is the relationship it has with customers, suppliers and competitors. A continuous strategic diagnosis helps to determine the changes that have to be made to a firm's strategy and internal capability in order to assure the firm's success in the turbulent environment.

Environmental Turbulence is a combined measure of the changeability and predictability of the firm's environment. Changeability is measured by the degree of complexity of challenges while predictability is measured by rapidity of change, Visibility of the future and Organization Capability.When the level of environmental turbulence changes, the historical organizational capability may become a major obstacle to the organization ability to adapt to the new challenges (Ansoff and MacDonnell, 1990).

Ansoff and MacDonnell (1990) presented the strategic success factors as follows: Aggressiveness of the firm's strategic behavior needs to match the turbulence of its environment, responsiveness of the firm's capability matches the aggressiveness of its strategy and the components of the firm's capability must be supportive of one another. The capability of a firm is determined by its resources (Pearce and Robinson, 2011). Challenges in the environment call for real time response throughout the year by detecting surprising changes and taking appropriate action as and when the need demands, increasing time for response to be able to manage and monitoring the rapid changes. In responding to the turbulence in the environment, it is not necessarily that periodic planning systems are disrupted. They can only be modified through monitoring and evaluation process.

The business environment continues to be driven by technological changes, globalization, and competition, products and customer satisfaction. As a result

organizations are to craft and implement strategies that ensure they stay relevant and successful. The environmental changes may occur rapidly or slowly, with or without a warning, they may be complex to some organization than others. Their impact on organizations choice of strategy may range from small to big, it is imperative for the organizations to have a watchful eye on those changes, the management must be alert for potentially important environmental changes, assess their impact and influence and adapt the organization's direction and strategy needed Thompson et al (2007).

2.3 Response strategies

Response strategies are a set of decisions and actions that assist organizations achieve their goals and objectives. They should be revised periodically in order to address the environmental challenges (Ansoff and MacDonnell, 1990; Pearce and Robinson, 1991). Responses strategies are either strategic or operational (Thompson and Strickland, 1993). Strategic responses are concerned with setting goals and objectives and maintaining a set of relationships that match organization capabilities and responsiveness to the environment. They create a position that assures present and future environmental viability and survival of an organization (Pearce and Robinson, 2011).

Operational responses are concerned with utilizing existing resources of an organization to counter environmental challenges (Johnson and Scholes, 2002). Competitive advantage is achieved when resources that are exclusive owned by a firm are applied to developing unique competences. Operational response strategies exploits the present strategic position of an organization by bringing out levels of outputs that will best contribute to achievement of the goals and objectives. The contributing activities to operational response are purchasing, human resource,

research and development, manufacturing, distribution and marketing. Response strategies to fraud are crafted by organization after considering its size and complexity. The response strategies include Fraud risk assessment, fraud reporting, Fraud investigation, governance, fraud detection, prevention, and control measures (IIA, ACFE and AICPA, 2008; ACFE Report, 2011; KPMG survey, 2010).

Fraud risk governance strategies involve putting in place, a risk management program that convey the expectations of the top-level management regarding fraud. Fraud governance strategies serve as the foundation for preventing, detecting, and deterring fraudulent acts by creating an environment where making the right decision is implicit. The organization's overall tone at the top sets the standard regarding its tolerance to fraud by ensuring implementations of policies that encourage ethical behavior from all stakeholders and monitor the effectiveness of fraud risk management program on a regular basis (HM treasury report, 2003; IIA, ACFE and AICPA, 2008; KPMG fraud and misconduct survey, 2010).

Fraud risk assessment strategies help an organization to understand fraud risk that directly or indirectly apply to the organization. A structured fraud risk assessment tailored to the organization's size, complexity, industry, and goals, should be performed and updated periodically (HM Treasury report, 2003). Risk assessments involves identifying risks, risk likelihood and risk response. Risk identification involves gathering information from all stakeholders that assist to determine incentives, pressures, and opportunities to commit fraud (Wells, 2007). Fraud risk assessment considers access and override of system controls by management as well as internal and external threats to data integrity, system security, and theft of financial and sensitive business information (Norton, 1994; IIA, ACFE and AICPA, 2008; ACFE Report, 2010).

Fraud detection responses are designed to identify fraud or misconduct that is occurring or has occurred; it involves examination of the facts to identify the indicators of fraud that warrant an investigation (Cheptumo, 2010). The fraud detection techniques should be flexible and adaptable to meet the various changes in fraud risk. The tools used to detect fraud in an organization are Audit review, management review, whistle blowing, process controls, and proactive fraud detection procedures (IIA, ACFE and AICPA, 2008). Whistle blowing is effective in organizations having a well-defined policy to protect whistle blowers. Internal Auditors are able to detect fraudulent practices especially in financial statement and bring this to the attention of management. Process controls are designed to detect fraudulent activity, as well as errors in operative processes. Proactive fraud detection procedures such as data analysis, continuous auditing techniques, and other technology tools can be used effectively to detect fraudulent activity by identifying anomalies, trends, and risk indicators within large populations of transactions. Effective detective controls are one of the strongest fraud deterrents (KPMG white paper, 2006; IIA, ACFE and AICPA, 2008; ACFE Report, 2010).

Fraud prevention strategies consist of all actions, policies, procedures, training, and communication that stop fraud from occurring. Setting up and implementing a strict internal control is vital in preventing fraud. The internal controls are meant to safeguard assets of the firm, ensure accuracy and reliability of accounting records and information, and promote efficiency in the firms operations and to measure compliance with the management prescribed policies and procedures (Brownbridge and Harvey, 1998). Weak internal controls have been cited as root causes of most occupational frauds (ACFE Report, 2010). The preventive strategies comprise analysis of human resource (HR) procedures, authority limits and transaction level

procedures. HR function ensures people hired are of good credentials, integrity and competence. Authority limit ensures approval levels of authority for employees match with their level of responsibility. Transactional level procedure reviews third party transactions to prevent the back-end fraudulent activities. Others prevention strategies are awareness and minimizing opportunities to commit fraud (Wells, 2007; IIA, ACFE and AICPA report, 2008).

Fraud investigation involves an in-depth analysis of fraud indicators by gathering sufficient evidence about a discovered fraud using an investigation team to ascertain occurrence of fraud. The investigation team should have necessary authority, knowledge and skills to evaluate the allegation and determine the appropriate course of action. The team should be mandated to report violations, deviations, or other breaches of the code of conduct or controls, regardless of where in the organization, or by whom, they are committed and impose appropriate punishment and suitable remedial action in a timely manner. Every organization should develop a system for prompt, competent, and confidential review, investigation, and resolution of instances of noncompliance and allegations involving potential fraud (KPMG white paper, 2006;IIA, ACFE and AICPA, 2008).

A consistent process for conducting investigations can help the organization mitigate losses and manage risk associated with the investigation. Where certain actions are required before the investigation is complete to preserve evidence, maintain confidence, or mitigate losses, those responsible for such decisions should ensure there is sufficient basis for those actions and the actions taken should be appropriate under the circumstances and applied consistently to all levels of employees. A suspect

should not be confronted until supporting evidence has been gathered (HM Treasury managing the risk of fraud, 2003).

Fraud risks affect all organizations. A proactive approach to managing fraud risk is essential in minimizing exposure to fraudulent activities. A combination of effective fraud risk governance, a thorough fraud risk assessment, strong fraud prevention and detection, as well as coordinated and timely investigations, can significantly reduce fraud risks. The changing environments of any organization require a continuous reassessment of fraud exposures and responses.

2.4 Concept of fraud and related challenges

The term fraud commonly includes activities such as theft, corruption, conspiracy, embezzlement, money laundering, bribery and extortion. Bank fraud refers to all forms of frauds committed against banks either by people from inside or outside the bank (wells, 2007). The effect of frauds can be seen in the downfall of entire organizations, massive investment losses, significant legal costs, incarceration of key individuals, and erosion of confidence in capital markets of countries, damage to reputations, brands, and images of many organizations around the globe. The major types of fraud affecting banks are Asset misappropriation, accounting fraud, bribery and corruption fraud, cybercrime, money laundering, tax fraud, illegal insider trading and sustainability fraud (PWC Global Economic crime survey, 2011).

A 2007 Oversight Systems study discovered that the primary reasons why fraud occurs are “pressures to do ‘whatever it takes’ to meet goals” (81 % of respondents) and “to seek personal gain” (72 %). Wells (2007) noted that people commit fraud when they have a motivation, can justify the activity and an opportunity exists. A 2010 and 2011 KPMG Singapore, Australia and New Zealand fraud survey identified

weak preventive measures, greed, poor leadership organization culture and lifestyle as causes of fraud. The survey also identified employees as being responsible for the largest proportion of fraud incidents closely followed by externals.

When fraud occurs, organizations deal with it in many ways, A 2011 PWC Global Economic Crime Survey revealed some of the ways organization use to deal with perpetrators are firing the employees involved (77% of respondents), informing police (44%), civil action (40%), doing nothing (4%), staff transfer (4%), warning (18%) reporting to relevant regulatory authorities (40%). A 2010 KPMG Fraud and Misconduct Survey, Australia and New Zealand, where the response was reporting the matter to police, launching an internal investigation and immediate dismissal of the staff, supported this.

The banking sector faces a number of challenges in their fight against fraud risk, this are dilemma of reporting fraud, organization perception of fraud, management involvement, Judicial systems and technology. Banks are hesitant to report fraud due to perceived damage to their reputation and exposure of their internal controls to public scrutiny (Norton, 1994, PWC Risk Survey, 2011). A 2010 KPMG Fraud and Misconduct Survey for Australia and New Zealand, had respondents saying that fraud cases are not reported to the police because they are regarded as minor crimes, or no money was lost, the fraud occurred overseas or reporting was overruled by the board of directors or the board audit committee.

The Judiciary systems are poorly equipped and incapable of bringing perpetrators of fraud to trial, the jury lack knowledge and experiences required to prosecute fraudsters (Norton, 1994). Judiciary systems in eastern Africa currently do not provide a significant deterrent to fraud. Systems are slow and the fines are small

compared to the value of fraudulent activities. Law enforcement authorities are poorly equipped to deal with white-collar crimes like bank and insurance fraud (PWC Risk survey, 2011). There is a need for greater education and awareness in this area.

The organization perception of fraud has been wanting on many fronts, According to a KPMG Fraud and Misconduct Survey 2010, Australia and New Zealand, only 20% of the respondents believed fraud is a significant problem for their own organizations, this prevailing attitude, particularly after many well publicized large frauds during the global financial crisis, will result in lower investment in fraud risk management and inevitably an increase in the level of fraud. The role of management to curb fraud has also not been clear. A 2010 ACFE report to the Nation indicated that the management should set the tone of no tolerance to fraud and communicate the same across the organization. A 2011 PWC survey revealed that some senior executives did not know if their organization had suffered a fraud.

Most organizations have inadequate attention to and understanding of fraud, a 2011 KPMG Singapore Fraud Survey revealed that most organization were not familiar with the red flags of fraud, some had weak management and board oversight and the staff did not understand their role in fraud prevention. This suggests that beyond the problem of many people not knowing how to identify or respond to fraud, there are also organizations where there is laxity towards fraud. Organizations need to be vigilant and proactive when fighting bank fraud. New types of fraud are emerging – cybercrime in particular. With new ways of doing business, new technologies and changing work environments, come new risks and new ways for fraudsters to carry out crimes. Organizations need to be aware of these changes and adapt their response strategies accordingly.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter details the various stages and phases of how the proposed study was carried out. It covers the design that was used to conduct the study, how data was collected and eventual analysis of the data in order to generate research findings for reporting. Therefore this section identifies the research procedures and techniques that were used in collection, processing and analysis of data. Specifically the following subsections are included: research design, data collection instruments, data collection procedures and data analysis.

3.2 Research Design

The research design used was a case study since the unit of analysis was one organization. A case study was used because it enabled the researcher to have an in-depth understanding of effectiveness of the response strategies to fraud adopted by Co-operative bank of Kenya. A case study design is most appropriate where a detailed analysis of a single unit of study is desired as it provides focused and detailed insight to a phenomenon that may otherwise be unclear (Mugenda and Mugenda, 2003).

The importance of a case study is emphasized by Young (1960) and also by Kothari (1990) who both acknowledge that a case study is a powerful form of qualitative analysis that involves a careful and complete observation of a social unit, irrespective of what type of unit is under study. It's a method that drills down, rather than cast wide.

3.3 Data Collection method

The study made use of both primary and secondary data. Primary data was obtained from managers at the Cooperative bank of Kenya using an interview guide. The interview guide (Appendix II) was used to collect data on types of fraud encountered by the bank, response strategies to manage fraud and their effectiveness. The data was collected from six (6) senior managers of the cooperative bank of Kenya holding key positions as far as managing fraud is concerned. The data collection method used was personal interviews. The interviewee guide with open-ended questions was used. Personal interviews enabled the researcher to administer oral questions in a face-to-face encounter that allowed collection of in depth qualitative data.

Secondary data was collected by use of desk search techniques from published reports of the bank, Kenya Bankers Association, Kenya credit and debit card fraud forum, Banking Investigation and Fraud Unit of Central bank, association of certified fraud examiners reports, Price Waterhouse coopers survey, Ernst and Young and KPMG survey reports.

3.4 Data Analysis

The data collected was qualitative in nature and was analyzed using content analysis, which is the best-suited method of analysis for a case study. According to Mugenda and Mugenda (2003), content analysis is systematic qualitative description of the composition of the objects of the study. The purpose of content analysis is to study existing documents in order to determine factors that explain a specific phenomenon. The researcher before analyzing examined the data for completeness, consistency accuracy and uniformity. The finding was presented in continuous prose as a qualitative report.

CHAPTER FOUR
DATA ANALYSIS, FINDINGS AND DISCUSSION

4.1 Introduction

This chapter presents the findings, analysis and discussion of the data obtained in the field as set out in the research methodology of the study on the effectiveness of fraud response strategies adopted by co-operative bank of Kenya. The data was gathered exclusively from an interview guide that was designed in line with the objectives of the study. To enhance data quality unstructured propping questions were used where by interviewees were free to indicate their views and opinion.

4.2 Types of Fraud

The study sought to determine whether fraud is encountered in the Co-operative bank of Kenya. All the six interviewees of the study indicated that fraud is encountered in the bank, the fraud comes in various forms and types and impacts negatively to the image and reputation of the bank. The interviewees also indicated that fraud is committed at all levels of operations and the perpetrators are both internal and external.

The study sought to determine the various types of fraud encountered by the Co-operative bank of Kenya in their operations. All the interviewees of the study identified the following types of fraud; payment card fraud, identity fraud, cheque fraud, loan application fraud, staff fraud, bank robbery, Internet fraud, accounting fraud, asset misappropriation, account take over, ATM fraud and Mobile Banking fraud. When the interviewees were asked to identify the most frequent fraud types, they indicated payment card fraud, mobile banking and Internet fraud. Bank robbery,

loan fraud and asset misappropriation were identified as being the leased frequent fraud types.

The interviewees were asked to identify the factors that contributed to the occurrence of the most frequent fraud types; they indicated that advancement in technology was main cause of escalating fraud cases in the bank. The technologies that enhance provision of better services to customers also provide opportunities for fraudsters to commit their crimes. Other causes of fraud were weak internal controls, poor HR practices ranging from recruitment, training and remuneration.

The interviewees were also asked to indicate the effects of fraud in their organization, they indicated that fraud is very sensitive and if not well managed, the effect would be downfall of organization, tainting of corporate image and reputation through bad publicity and financial loss to the company. The interviewees feared that bad publicity would lead to loss of customers' trust and goodwill.

When the interviewees were asked why payment card, mobile banking and internet fraud were most frequent, they indicated that they are easier to commit, the perpetrators don't need to be present while committing them for instance the case of card not present transaction for payment cards that are done online. For mobile banking the fraudsters only require a mobile PIN that can easily be obtained from a customers phone since most customers store such information as contacts on their phones.

The study also sought to investigate why bank robbery was least frequent, the interviewees indicated that banks have put in place elaborate access controls measures that deter such fraud, for instance safe vaults have a multiple locks whose keys and access codes are held by different people. Furthermore all access points have security

cameras while cash carrying vehicles are escorted by well-armored police officers. The interviewees were also asked to identify which fraud types had caused the largest financial loss to the bank. Among the most frequent types of fraud they identified card fraud as having led to a huge loss to the bank. They were also asked to identify the major card fraud that the bank has encountered and they indicated stolen and lost cards, counterfeits, Card not received and card not present fraud.

4.3 Response strategies to fraud

Strategic responses are set of decisions and actions designed to achieve objectives of an organization. This study sought to establish the response strategies to fraud as adopted by the co-operative bank of Kenya. Based on the response from the interviewees', the following are fraud response strategies practiced at Co-operative bank of Kenya. The interviewees indicated that the bank has a well-documented fraud policy in operation. The fraud policy outlines the strategic direction, priorities, goals and objectives for managing fraud risk. The policy sets out the blueprint for fraud prevention, detection, investigation, control and governance for the bank.

The interviewees indicated that regarding staff fraud, new employees are required to submits certificate of good contact to Human resource before they are confirmed, the bank also obtains commendation letter from the referees and former employers for those who were in employment. This documents helps the bank to vet the integrity of new employees. The interviewees further indicated that the employees are informed of the anti fraud policy which is incorporated in the business code of conduct, on a yearly basis they are required to sign a declaration of secrecy policy documents. The bank also maintains a transaction level limit for all tellers where by cash withdrawals and deposits beyond a certain amount will refer for approval before posting.

The study established that the bank has a 24-hour team that is charged with the responsibility of monitoring all incoming and out going transaction in the bank systems. In cases of abnormal transactions, the officer on duty is empowered to contact the customer to verify the authenticity of transaction, stop further transactions on the account and refer the case for further investigation. The bank also has in place relationship managers in various units to give specialized service to corporate clients the managers are required to have a deeper understanding of all customer businesses.

The interviewees indicated that the bank has invested heavily in advanced in technology to manage fraud, technology has made risk monitoring easier by making it possible to obtain tailor made reports and carry out trend analysis for suspected fraud. The reports are generated based on a set of parameters such as amounts, merchants, and frequency of transactions. The parameters are revised from time to time depending on nature of fraud in the market.

The study established the bank has a clear fraud reporting and investigation lines, a suspicious activity in any business unit is reported to the business unit head, the unit head collects all material facts and refers the case for full investigation and recommendation to the Head of Security Department. The security department carries out full investigation of the case and writes a report that is presented to Board of management for adoption, once adopted, the business unit head is advised of the findings and recommendations. The bank has a contact Centre manned by several executives where customers can call to report suspicious activity on their accounts or a breach in our bank systems. The contact Centre executive collects all reports and forward to relevant unit for further action on case-by-case basis.

The interviewees indicated that in order to manage internet fraud, the bank has made it mandatory for any customers wishing to transact online to fill an internet access form from the branches, the branch officer confirms the client details and send the form via email or dispatch to head office, upon receipt of the form at head office, the form is again checked and the card enabled, the internet access form indemnifies the bank against any unprecedented losses. To protect customers from losses, the study established that the bank has restricted access to suspicious websites and online merchants, through technology it has secured all web applications against common malware attacks and ensured periodical software updates.

The interviewees indicated that the bank response to cases of identity theft through implementation of know your customer policy (KYC) .The policy involves full verification of documents at point of account opening by bank officers, the bank officers compares the original documents and copies as provided by the customer, the authenticity of original documents is checked via the UV light. The documents are again checked later in the day by back office operation team after which upon satisfaction an account is opened. It is also a requirement that all new customers must present themselves at the Branch level where all KYC is done.

The study established that in order to curb cheque fraud, the bank has set transaction limits for respective members of staff. The transactions limits provide guidelines to the value of cheques employees are allowed to write and cash. The authority vested in the employee determines the transaction limit. High valued cheques require a senior manager to authorize; the bank does a call back to drawer of the cheque before making payment to establish that it is in order. The bank has also embarked on full training of all its employees dealing with cheques on security features on cheques.

The study established Bank robbery is managed through strict internal access control, there is an access control to safe vaults and bank premises, every person entering into the bank premises must have an identification tag, the guards from well established security firms have been engaged to man all entry and exits points for all bank premises. There is also an alarm systems linked to the Kenya police Hotline that gives alerts whenever there is a breach in security systems. It was established that opening of safe vault requires at least three people who hold different combination of access codes.

The study established that all onsite Automatic Teller Machines (ATM) are fitted with surveillance camera's that captures all activities in the lobby, the recorded details helps in cases of fraud. The ATM lobbies are managed by security guards who are mandated to reports suspicious activities at the ATM for full investigations. The bank also has made available several posters at entrance and inside ATM lobbies that inform customers of security measures they need to know while using their payments cards.

Regarding the response strategy to M-banking fraud, the interviewees indicated that the bank's m-banking platform encrypts all outgoing messages making it difficult for fraudsters to access outgoing messages, the internal customer data is also encrypted to limit access by all members of staff. The decrypting rights are only limited to authorized members of staff. In addition the customers an SMS alerts is automatically send to a customer for all successful transactions done, the customers choose the nature of alerts they receive when opening an m-banking account. The bank has also set daily limit for M-banking transactions.

The study established that the bank works in collaboration with other banking institutions in managing the risk of fraud by sharing information. Fraud cuts across all sectors of the economy, it is important that information on frauds is shared to assist reduce repeat frauds, it was established that there is banking fraud forums organized by Central bank of Kenya where all matters relating to fraud are discussed and strategies developed to counter effects of fraud. The bank as a member of the forum shares fraud information and gets informed of frauds trend across the banking sector.

The interviewees indicated that the board of management at the bank is fully involved in management of fraud. The Board is charged with the responsibility of establishing fraud governance strategies that serve as the foundation for preventing, detecting, and deterring fraudulent acts. The Board creates a favorable environment where managing risk of fraud is possible within an organization. Governance strategies sets the organization standard regarding its tolerance to fraud by ensuring implementations of policies that encourage ethical behavior from all stakeholders and monitor the effectiveness of fraud risk management program.

4.4 Effectiveness of fraud response strategies

The study sought to investigate the effectiveness of fraud response strategies adopted by the Co-operative bank towards fraud risk, with regards to KYC policy it was established that it is the most robust and effective method that can be used to deter fraudster's, a well done KYC will ensure only valid and quinine customers are allowed to open accounts with the bank. The KYC enable the bank to have an in depth knowledge of the nature, character and integrity of their customers and creates a closer relationship.

With regards to the 24-hour risk monitoring, the interviewees indicated that this method has reduced to a great extend the occurrence of fraud, it has assisted in establishing fraud trends, common points of compromise and weak points in the systems that are likely to be exploited by the fraudsters, the method has acted as an early warning alert that has minimized the extend of loss to the bank. Risk monitoring officers are well equipped to advise the bank on new trends of fraud and set systems parameter accordingly.

The study sought to investigate effectiveness of response strategies to internet fraud, the interviewees indicated that requesting the customers to apply for internet access rights to use their payments cards has reduced the loss to the bank and shifted the responsibility for risks to the customer, the customers are now very careful when transacting online since they are aware that they are liable should their accounts be compromised. Restricting access to suspicious Internet websites has served as an alert to customers to websites that expose them to risk of fraud.

The study sought to investigate the effectiveness of having a fraud policy in managing fraud, the interviewees indicated that presence of a fraud policy has brought awareness to all members of staff on procedures and guidelines to be followed whenever fraud is discovered to at any levels in an organization, this has shortened the response time to management of fraud. The policy has given direction and framework on which fraud cases are to be handled and who takes responsibility. The interviewees however indicated that on its own a fraud policy does not deter, prevent or control fraud, its level of effectiveness is determined by how well it is implemented by an organization.

The study sought to determine the effectiveness of access control to bank systems and premises; the interviewees indicated that access control to bank premises has deterred fraudsters since they fear being caught on surveillance camera and being identified by security officers at the entrance. Access to bank systems is through user name and password and every member of staff is directly held accountable for the use of their passwords. The bank is be able to trace the movement of a person whose access code was used to enter a premise or bank systems and any unusual access is investigated immediately by the security team.

The study also sought to determine effectiveness of strict recruitment process as a response strategy to staff fraud, the interviewees indicated that effective recruitment process has led to reduced incidences of fraud committed by bank employees, requirement of certificate of good conduct, recommendation letter from referees, aptitude test and intelligent test from new recruits ensures that people hired are of good credentials, integrity and competence. Furthermore this process scares fraudsters from applying for employment opportunities in the bank.

The study sought to determine effectiveness of using advanced technology to manage fraud, the interviewees indicated that proper and advanced systems are effective in detecting, preventing and controlling fraud, modern systems have the capability to analyze historical data based on preset parameters and generate reports that assist in identifying the fraud trends, common weak points in organization and possible solutions or mitigating factors. The advanced systems have embedded security features at every stage of development making it hard for fraudsters to commit crimes. New technology allow for modification to address emerging security threats unlike old technologies.

The study sought to investigate the effectiveness of fraud reporting and investigation strategies in Co-operative Bank of Kenya, the interviewees indicated that a clear reporting channels and a consistent process for conducting investigations has helped the bank mitigate losses and manage risk associated with fraud. Fraud investigation team in the bank does an in-depth analysis of fraud indicators by gathering sufficient evidence about a discovered fraud and ascertains if indeed fraud has occurred. The findings of investigation team has assisted in revealing violations, deviations and breaches of the controls, regardless of where in the bank, or by whom, they are committed and impose appropriate punishment and suitable remedial action in a timely manner.

The study sought to investigate the effectiveness of fraud governance strategies employed by the bank to manage fraud, the interviewees indicated involvement of board of management to manage fraud has been fruitful, the board contribution has been in allocation of the resources critical in fight against fraud and setting an overall tone to all stakeholders on the standard regarding its tolerance to fraud by ensuring implementations of policies that encourage ethical behavior from all stakeholders and monitoring the effectiveness of fraud risk management program on a regular basis. The position taken by management regarding its tolerance to fraud has served, as a clear warning to all would be fraudsters that fraud is not tolerated in the bank.

4.5 Discussions of Findings

The findings of this study established that poor HR practices are partly to blame for escalating fraud cases by employees. Employees know the weaknesses in an organization and if not well handled May lead to large loss to an institution. The findings of this study are consistent with a previous study done by Cheptumo (2010)

on response strategies to fraud related challenges at Barclay's Bank where employee screening was critical in fight against internal fraud. This study recommends adequate revision of hiring practices to include integrity tests, checking names with Credit Reference bureau for credit worthiness, strict internal access controls to bank premises and systems, training, restricting use of smart phones in bank premises and monitoring all email communications in addition to traditional practices in place.

The advancement in Information technology has brought conveniences that have influenced modern communication, financial dealings, travel, security and commerce. However this gain has brought about vulnerability, risk of abuse, intentional manipulation and sabotage of banking networks. The findings of this study established that the bank's technology has assisted in managing risk of fraud. The study recommends that better-qualified internal and external Auditors working in liaison with the police officers can handle technology based fraud adequately; the Auditors who understand bank operations and are able to pinpoint weak points and suggest ways of sealing the loopholes. A previous study done by Wanjiku (2011) on Strategic Response of Equity Bank to Fraud Related Risks identified the critical role of Auditors in controlling fraud.

The findings of this study suggest that banks should embed security features early on ICT projects rather than wait at launch stage. This would avoid the last minute rush that end up allocating more access rights to some users than they require thereby opening up loopholes where business data is transferred to other external entities that cause future vulnerability. Security features be treated as a functional requirement rather that just a technical one. The information security requirement should be captured at blue print stage of every project. The study further recommends that banks

data back-ups that is done daily after end of day operations, should be done on hourly basis to avoid the risk of loosing a day's data that may never be recovered.

The findings of this study identified that a fraud policy gives a guidelines on how fraud is to be managed, this reduces the response time since action taken within a few hours of discovering fraud is critical in an organization effort to manage effects of frauds. The study recommends that fraud policy should be updated on a regular basis to capture emerging trends of fraud cases and ensure the bank is a head of fraudsters. This finding is also consistent with a study by Wanjiku (2011) on Strategic Response of Equity Bank to Fraud Related Risks where she identified fraud policy as a blue prints that guides how fraud cases are managed at every business unit level.

The findings of this study established that risk monitoring at all levels reduces the incidences of fraud. The monitoring team is charged with the responsibility of monitoring all transaction in the bank systems and take remedial action in cases of abnormal transactions. The team has assisted in identifying early warning signs for fraud, weak areas in bank systems and access controls that are likely to be exploited by fraudsters. The study recommends empowerment of monitoring team with resources to assist them take quick remedial action and stop further fraud. The line managers should from time to time make a random check to this team especially at night to ensure that they are doing duties assigned to them. A study by Cheptumo (2010) on response strategy to fraud related risks at Barclays Bank identified risk 24-hour monitoring as being effective in raising the red flags for unusual account activities.

The findings of the study established that all customers intending to transact online must request for their payments cards to be enabled. The bank has restricted access to

suspicious websites and web applications. Internet fraud forms such as electronic money laundering has been aided by development of informal banking institutions that bypass Central Bank of Kenya supervision provision for cash transaction and Electronic cable vandalism that cause a lot of damage to banks. The study recommends legislation to allow Central bank supervision provision to be extended to informal banking institutions. The banks should collaborate with Telkom companies regarding security of cables network and educate customers on common Internet security threats and practices that facilitate occurrence of fraud.

Payment card fraud takes the form of card skimming, card trapping, counterfeit, lost and stolen cards, card not received and card not present. Fraudster use specialized gadget to capture cards at ATMs and card data on magnetic strip that is later used to commit fraud. The findings of the study established the bank does monitoring of all cards transactions, has restricted use of payment cards in specific countries and merchants and by default deactivated debit cards from online transaction. These measures have played a critical role in reducing occurrence of fraud. The study recommends a shift to chip enabled cards that have higher security features compared to the magnetic strip cards currently in circulation.

The findings of the study established that the bank maintains know your customer (KYC) policy to manage identity fraud. The policy involves full verification of documents at point of account opening by bank officers who verifies the authenticity of the original documents as provided by the customer. The findings are similar to those of a study by Njagi (2009) which looked at effectiveness of know your customer policy adopted by commercial banks in reducing money laundering, in his findings banks that fully complied with the policies reported few cases of fraud. The study recommends that the policy should include checking names with the Credit

reference bureau for credit worthiness of the customers. The government should make it mandatory for all citizens to acquire the new generation National ID that has advanced security features since banks mostly use the National ID as the main identification documents during account openings.

The findings of the study established that the bank manages cheque fraud by setting transaction limits for respective members of staff. The transactions limits ensures that a member of staff is only allowed to write or pay a cheque whose value is in line with her authority and power, The study further recommends the bank to embark on full training of all its employees on security features on cheques. The bank must shift to cheque truncation process where a machine is used to capture cheque details for foreign banks and details send to respective banks to confirm authenticity before payment is done. This will reduce occurrence of fraud.

The findings of the study indicated that a strict access control to safe vaults and bank premises is maintained. The study recommends that the bank should take an active role and work in collaboration with security firms in training the security officers assigned at their premises due to nature of activities that bank does, the officers should receive additional training on bank security and their welfare taken care of to avoid situation of complacency and compromise.

The findings of the study established that offside Automatic teller machines (ATM) are frequently affected by fraud, the bank has managed to fit security camera's in all onsite ATMs and is in the processes of doing the same to offsite ATMs. The ATM lobbies are managed by security officers who are mandated to reports suspicious activities at the ATM for full investigations. The study recommends settings all ATMs in open places to public to avoid mugging and fraudsters taking their time to

install cash trapping gadgets and other devices that capture customer details, all lobbies must be fitted with surveillance cameras to discourage fraud.

M-banking services has made it easier for customers to make banking transaction using their mobile handsets. The findings of the study established that the m-banking platform encrypts all outgoing messages and sends transactions alerts to customers. These measures are currently working but more needs to be done. The study recommends that customers be mandated to block the service at press of a button on their phone whenever they suspects fraud, the bank should educate customer's on common safety practices education that safeguard their details such as PIN. Monitoring mobile money transfer will ensure the platforms are secured from cyber criminals.

The study established that sharing of information is critical in fight against fraud; Sharing of information reduces replication of frauds types between sectors, economies and countries. The findings of the study indicated that the Central bank of Kenya has a unit that brings together all stakeholders in the banking sector to share information on fraud. The study recommends establishment of fraud forums for all sectors to consolidate efforts to counter effects of fraud. Their is need to establish a fraud response Centre in the country whose mandate would be to coordinate, gather, liaise, disseminate technical information on fraud, carrying out research and analysis and capacity building in fraud management.

The management of fraud depends on the goodwill from the senior management in banking sector. The finding of this study established that the management view regarding fraud determine the strategic approach taken by the banking sector. Where the management is aware of effects of fraud, they set strategies that serve as the

foundation for preventing, detecting, and controlling fraudulent acts. The study recommends involvement of top-level management on daily basis, the security team should directly inform the top-level management on fraud situation to hasten immediate remedial action.

With regard to reporting and reward for employees and customers who assist in frustrating fraud, the study established that staffs are given commendation letters after a successful frustration of fraud by head of business units. This letters are put in individual files and may be considered in in future promotion for the employees. The study revealed that even though whistle blowing is entrenched in the fraud policy, there are no designated boxes where customers and employees can report fraud incidences secretly. The study recommends establishment of dedicated telephone lines, SMS lines, boxes and email address in all bank premises to encourage whistleblowing.

The study further recommends direct involvement of the government especially in legislating laws to deal with fraud; the penalties for committing fraud under the current laws on all types of fraud are lenient. Lack of statutory structure to address this challenges complicate the investigations and prosecution of fraudsters. The police force reforms should be done to ensure police officers are fully empowered to investigate and prosecute fraudsters. Reforms in judiciary would ensure only properly trained magistrates able to determine the gravity of fraud and impose adequate sentences are assigned to fraud related cases. Previous study by Wanjiku (2011) also recommended reforms in judiciary and police force to enhance fight against fraud.

CHAPTER FIVE
SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter seeks to provide a summary of the findings of the study and also draw conclusions and recommendation to address the objective of the studies which was to determine effectiveness of fraud response strategies adopted by Co-operative bank of Kenya.

5.2 Summary of Findings

The first objective of this study was to identify the types of fraud encountered at co-operative bank of Kenya. The study identified the following fraud types: Identity fraud, card fraud, cybercrime, ATM fraud, internet fraud, Mobile Banking, staff fraud, bank robbery and accounting fraud.

The second objective was to identify response strategies to fraud employed by co-operative bank of Kenya. The study identified the following strategies: real time monitoring, know your customer policies, Auditing, advanced technology, training, employee screening, internal system controls, access control, data security, fraud investigation and reporting, sharing information in fraud forums and fraud Policy framework.

The study found out that staffs are properly screened before they are offered full employment, new employees are put on probation for six month, required to submits certificate of good contact to Human resource before they are confirmed, the bank also obtains commendation letter from the referees and former employers for those who were in employment. The new staff are made aware of the anti fraud policy which is incorporated in the business code of conduct, on a yearly basis the they are

required to sign a declaration of secrecy documents that binds and hinders them from divulging any internal sensitive information.

The study found out that even though whistle blowing is entrenched in the fraud policy, there are limited facilities such as boxes in designated places where customers and employees can report secretly, all existing boxes are located in open arrears and therefore discourages employees and customers. The study found that the bank has embraced technology to enhance service delivery, technology has made risk monitoring easier, it is now possible to obtain tailor made reports and carry out trend analysis for suspected fraud. The reports are generated based on a set of parameters such as amounts, merchants, and frequency of transactions. The parameters are revised from time to time depending on nature of fraud in the market.

The study established that the bank has a 24-hour team that is charged with the responsibility of monitoring all incoming and out going transaction in the bank systems. In cases of abnormal transactions, the officer on duty is empowered to contact the customer to verify the authenticity of transaction, stop further transactions on the account and refer the case for further investigation. The bank also has relationship managers in various units to give specialized service to corporate clients. The study found out that a fraud policy exists at Co-operative Bank of Kenya, the fraud policy outlines the strategic direction, priorities, goals and objectives for managing fraud risk. The policy sets out the blueprint for fraud prevention, detection, investigation, control and governance for the bank.

The study found out the bank maintains a know your customer policy (KYC) .The policy involves full verification of documents at point of account opening by bank officers, the bank officers compares the original documents and copies as provided by

the customer for authenticity. Back office operation team confirms further customer details before opening the account in the bank system. It is also a requirement that all new customers must present themselves at the Branch level where all KYC is done, after which they can now open other accounts with the bank.

The study found out that the board of management is fully involved in management of fraud risk. Managing fraud requires resources and the board of management is responsible for allocation of the overall resources in an organization. The board also has developed fraud governance strategies that serve as the foundation for preventing, detecting, and deterring fraudulent acts. The board of managements sets the overall tone regarding its tolerance to fraud by ensuring implementations of policies that encourage ethical behavior from all stakeholders and monitor the effectiveness of fraud risk management program on a regular basis.

The study established that sharing of information is critical in fight against fraud, fraud is universal and affects every sector of the economy in the same way hence a collective effort is necessary. Sharing of information reduces replication of frauds types between sectors, economies and countries and enables organization to take a proactive role in fight against fraud.

The findings of the study established that major challenges in fight against fraud are poor legislation, judiciary system and poorly equipped police force. The study recommends direct involvement of the government especially in legislation on laws to deal with fraud, development of statutory structure to assist investigations and prosecution of fraudsters. The study also recommends reform in the police force, reform in the judiciary to allow well trained magistrates who are able determine the

gravity of fraud and impose adequate sentences that will discourage fraudsters to handle cases of fraud.

The study found out that the current response strategies to fraud in the bank are effective especially on existing traditional fraud types, the strategies have managed to deter further occurrence of fraud cases, however new trends of emerging fraud are becoming a challenge, the commercial banks are required to devise new strategies with each emerging strains of frauds types otherwise over reliance on old strategies might result in financial losses to the bank.

5.3 Conclusions of the Study

Banks face unending task to detect, prevent and control occurrence of fraud on day-to-day basis. Fraud is persistent, and banks need to be vigilant and proactive when fighting fraud. 'Traditional' frauds like identity theft; staff fraud, atm fraud and bank robbery remain the top three frauds committed against banks. But 'new' types of fraud are emerging such as –cybercrime, card fraud and mobile money transfer fraud. With new ways of doing business, new technologies and changing work environments, come new risks and new ways for fraudsters to carry out crimes. Banks need to be aware of these changes and adapt their response strategies accordingly. The emerging fraud types are proving elusive and traditional strategies are not effective in stopping their occurrence, banks should constantly review all existing strategies for effectiveness in the wake of new types of fraud. Sharing information in fraud forums and regular training will enable frauds analysts to effectively fights criminals.

The major strategies that banks use to combat fraud are Real time monitoring, periodical Auditing, governance policies, training, know your customer, fraud

reporting mechanism, staff vetting procedures, use of advanced technology, strict internal controls, data security, sharing information in fraud forums and fraud Policy framework. Due to different types of fraud, the co-operative bank applies more than one strategy to combat fraud.

The bank needs to set up proper control measures with every adoption of new technology. The recruitment and training of members of staff needs to be considered since poorly motivated staff may be accomplices in fraud crimes. The challenges of fraud indicated were lack of modern technology to assist in fraud detection, lack of trained fraud analysts, lack of management support to fraud, weak internal controls, lack of code of conduct, lenient penalty for convicted fraud crimes and slow pace of fraud cases in our judiciary system.

5.4 Limitations of the Study

The study focused on commercial banks, it would be better if other non-bank institutions such as micro finance companies, savings and credit co-operative societies and forex bureau's were considered. The main respondents were senior managers of the bank who being normally busy had limited time for interviewee, junior employees who actually implement the strategies needs to be considered. The study also focused entirely on bank perspective, other stakeholders such as customers need to be considered. Time limitation made it impractical to include more respondents in the study.

5.5 Suggestions for further research.

The study focused on effectiveness of response strategy to fraud at Co-operative bank of Kenya. Further research needs to be done on challenges of implementing fraud

response strategies in the banking sector. A further research can be done on response strategies to combat technology-based fraud in the banking sector.

5.6 Recommendations for policy and practice

The current frauds causing the biggest financial loss to banks are as a result of advancement in technology. Fraudsters are constantly searching for loopholes in technological systems in order to cause harm to banks. Embedding security features at blue print stage on technology-based projects is important. The security systems should be incorporated at initial stages to avoid the last minute rush that end up allocating more rights to users than they require. Security features be treated as a functional requirement rather that just a technical one.

The study recommends reform in the police, judiciary and legislation, security features on identification documents, whistleblowing policy, and staff management. The study recommends a clear dissemination of fraud policy to all stakeholders in the bank; let it not be a preserve of the Risk managers. Internal fraud occurs due to lack of knowledge or laid out procedure for handling fraud. The recruitment and training of members of staff needs to be considered since poorly motivated staff may be accomplices in fraud crimes.

REFERENCES

Ansoff, H. & Macdonnell.(1990).*Implanting Strategic Management* (2nd ed.). London: Prentice Hall.

Ansoff, I. (1988). *Corporate Strategy*. Boston: Prentice Hall.

Apostolou B, H. J. (2001a). Management fraud risk factors:rating by forensic experts. *The CPAJournal* , October,48-52.

Association of Certified Fraud Examiners(ACFE). (2006). Report to the Nation on Occupational Fraud and Abuse. www.acfe.com.

Association of Certified Fraud Examiners(ACFE). (2010). Report to the Nations on OccupationalFraud and Abuse. www.acfe.com.

Brownbridge, M & Harvey C. (1998). *Banking in Africa*. Asmara: Africa World Press,Inc.

Central Bank of Kenya (CBK). (2011). *Annual Report*. Nairobi: Central Bank Of Kenya.

Central bank of Kenya (CBK). (November 2011). *Monthly Economic Review*. Research and Policy Analysis. Nairobi

Cheptumo, N. (2010). Response Strategies to fraud related challenges by Barclays Bank of kenyaUnpublished MBA project of The University of Nairobi.

Ernst &Young LLP. (2010).11th Global Fraud Survey,Driving ethical growth –New Markets,newchallenges. EYGM Limited.

Fitch, T. P. (1997). *Dictionary of Banking Terms* (3rd ed.).(D. G. Dr Irwin L Kellner,(Ed)New York: Barron's Educational Series,Inc.

Ford, N. (2011, 2nd Quarter). African Banker. (A. Versi, Ed.) Banking in East Africa (16), pp. 24-32.

Ford, N. (2011,1st Quarter).African Banker (A. Versi, Ed.) Banking Security-How to Beat Fraudsters (15), pp. 18-29.

Grant, R. (1998). *Contemporary Strategy Analysis* (3rd ed.). Massachusetts:Blackwell Publishers Ltd.

Mintzberg et al (1999). *The strategy Process*. Harlow, England:Pearson Education Limited.

HM Treasury. (2003, May). Assurance, Control, and Risk:Managing the Risk of Fraud:AguideforManagers,2003.Retrieved,May02,12,http://webarchive.nationalarchives.gov.uk/www.hm-treasury.gov.uk

IIA, ACFE, AICPA. (2008). Managing the Business Risk of Fraud: A practical Guide. www.acfe.com/publications.aspx.

John .D &, Jordan. E. (1995). *Dictionary of Finance and Investment terms* (4th ed.). New York: Barron's Educational Series,Inc.

Johnson G.& Scholes K. (2002). *Exploring Corporate Strategy*. New Delhi: Prentice-Hall.

KPMG. (2010). Fraud and Misconduct Survey 2010, Australia and New Zealand.kpmg,com.au.KPMG International.

KPMG. (2004).Fraud Risk Consideration-Audit Committee Roundtable Workshop-Spring 2004. www.kpmg.com

KPMG. (2006). Fraud Risk Management-Developing A strategy for Prevention,Detection and Response. http://www.kpmg.com.

KPMG. (2007). KPMG International. Retrieved 03 26, 2012, from www.kpmg.co.uk/pubs/ ProfileofaFraudsterSurvey(web).pdf

KPMG LLP. (2010, 08 11). Addressing the Risk of Fraud and Misconduct.Retrieved 2012,fromhttp://www.kpmg.com/NZ/en/IssuesAndInsights/ArticlesPublications/Documents/2010-Fraud-misconduct-survey.PDF

KPMG. (2011). The KPMG Singapore Fraud Survey Report 2011. http://www.kpmg.de.

Jihingan.M,&Jihingan.S.(1994). *Currency and Banking*.New Delhi:KONARK PUBLISHERS PVT LTD.

Mbwayo, M. (2005).Strategies applied by commercial banks in Kenya in anti money Compliance Programs. Unpublished MBA Project , University of Nairobi.

Nigel, D. (Ed.). (2010, 04). Quantum. Retrieved 03 26, 2012, from Quantum Magazine: www.quantummagazine.com/Quantummagissue11.

Njagi, L. (2009). Effectiveness of know your customer policies adopted by Commercial banks in Kenya in reducing money laundering and fraud incidences.Unpublished MBA Project,University of Nairobi.

NORTON, J. (1994). *Banks:Fraud and Crime*. (J. Lubbock, Ed.) LONDON: LLOYD'S OFLONDON PRESS LTD.

Obone, A. (1993). *Monetary theory,banking and public finance* (4th Edition ed.). Kampala:The Marianum Press.

Olive Mugenda and Abel Mugenda. (2003). *RESEARCH METHODS Quantitative and Qualitative Approaches*. NAIROBI: Acts Press.

Onoh, J. k. (1982). *Money and Banking in Africa*. New York: Longman.

Oversight Systems Report on Corporate Fraud, www.oversightsystems.com. (2007).

Pearce J.A& Robinson, J.(2011).*Strategic Management* (12 ed.) New York: Irwin MacGraw-Hill

PricewaterhouseCoopers International Limited(PwCIL).(2011).Global Economic Crime surveyCybercrime:Protecting against,the growing threat. www.pwc.com/crimesurvey:

PricewaterhouseCoopers Kenya Limited.(PWC). (2011). Risk Survey. www.pwc.com/ke.

Reuvid, J. (Ed.). (2010). *Managing Business Risk*. London: Kogan Page.

S.Majluf, A. C. (1996). *The strategy Concept and Process*. New jersey: Prentice Hall.

Shekhar, K. (1984). *Banking Theory and Practice* (Sixteenth Edition ed.). New Delhi: VAN EDUCATIONAL BOOKS.

Srikrishna, S. (2009, 03). Businessgyan.Retrieved 03 26, 2011,from www.businessgyan.com.http://www.businessgyan.com/node/5687

The Chartered Institute of Management Accountants(CIMA). (2010). Fraud Risk Management–A Guide to Good Practice. Retrieved 05 02, 2012, from http://www.cimaglobal.com

Thompson, et al. (2007).*Crafting and Executing Strategy* (15 ed.). New York: McGraw-HillIrwin

Thompson et al. (2006). *Crafting and executing strategy*. NEW DELHI:Tata Mcgraw-Hill Publishing Company Limited.

UK Financial Services Authority. (2006). Firms' High-Level Management of Fraud Risk. Retrieved on 05 02, 2012, from http://www.fsa.gov.uk.

Visa. (2011). Visa Europe *Annual Report*.

Wanemba, M. (2010). Strategies applied by Commercial Banks in Kenya to combat Fraud.Unpublished MBA project Of The University of Nairobi.

Wanjiku, L. (2011). Strategic Response of Equity Bank to Fraud Related Risks. Unpublished MBA project of the University of Nairobi.

APPENDICES

APPENDIX I: COVER LETTER

TIMOTHY WANYAMA**,**
University of Nairobi,
P.O BOX, 30197
Nairobi.
June 2012

Dear Sir/Madam,
RE: DATA COLLECTION

I am a postgraduate student at University of Nairobi undertaking a Master of Business Administration degree Program majoring in Strategic Management. One of my academic outputs before graduating is a research project and for this I have chosen the research topic "**Effectiveness of fraud response strategies adopted by Co-operative bank of Kenya limited**".

You have been selected to form part of the study. This is to kindly request you to assist me collect the data by responding to the interview guide. The information you provide will be used strictly for academic purposes and will be treated with utmost confidence.

A copy of the final report will be available to you upon request. Your assistance will be highly appreciated.

Yours sincerely,

TIMOTHY WANYAMA

APPENDIX II: INTERVIEW GUIDE

INTERVIEW GUIDE FOR MANAGEMENT STAFF IN SELECTED UNITS OF CO-OPERATIVE BANK OF KENYA

This interviewee guide seeks to collect information on response strategies adopted by Co-operative bank of Kenya to fraud related challenges and their effectiveness. Kindly provide honest answers to all questions asked. All the information will be treated confidentially and used for academic purposes only.

INTERVIEW QUESTIONS

1. Interviewee's managerial position.

2. Do you Encounter fraud in the bank.

3. What types of fraud do you encounter

4. For each of the fraud types above, what do you do to be able to deal with them?

5. How effective do you find each of the method mentioned above in managing fraud.

6. Do you also encounter the following types of fraud (those not mentioned in Q3)

THANK YOU FOR YOUR TIME AND COOPERATION.