STRATEGIC RESPONSE OF EQUITY BANK TO FRAUD RELATED RISKS

BY:

LOISE KINYUA WANJIRU

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

NOVEMBER, 2011
DECLARATION

STUDENT’S DECLARATION

This research project is my original work and has not been presented for a degree at any other university.

Name: LOISE KINYUA WANJIRU D61/60074/2010

Signature……………………………………… Date ………………………

SUPERVISOR’S DECLARATION

This research project has been submitted for examination with my approval as the candidate’s University Supervisor.

Name: JEREMIAH KAGWE

Signature ………………………………………… Date ………………………
DEDICATION

This study is dedicated to my loving family.
ACKNOWLEDGEMENT

I thank the Almighty God for His guidance and providence which enabled me to undertake this project that was too involving in terms of time and resources.

I wish to express my sincere appreciation to my family for their understanding and support during the project.

Lastly, I would also like to express my sincere thanks to the supervisor JEREMIAH KAGWE for having agreed to supervise this research paper and their patience in reading the drafts and occasionally guiding me, without which the research would not have been a reality.
ABSTRACT

Prior studies have found that failure to detect fraudulent financial reporting can expose the auditor to adverse legal and/or regulatory consequences. Most of them are on international scenes or on developed countries. At the time of the study, no local or international studies had ever focused on the strategic responses adopted by banks in Kenya to counter increasing fraud risks. This was despite the ever increasing cases of fraud risks that had claimed a number of financial institutions in Kenya and thus calling for strategic responses to curb the spread of the crime. The study generally sought to determine the responses by Equity Bank to fraud related risks in the banking industry.

This was a case study since the unit of analysis was one organisation aimed at getting detailed information regarding the strategic responses to increasing fraud related risks at Equity Bank of Kenya Limited. Primary data was collected using an interview guide. The interview guide contained open-ended questions. The open-ended questions enabled the researcher to collect qualitative data. Before processing the responses, the completed interview guide was edited for completeness and consistency. A content analysis was employed. The content analysis was used to analyze the interviewees’ views about the strategic responses to fraud risk in Equity Bank. The information was presented in a continuous prose. 18 out of the 20 interviewees targeted completed the interview guide making a response rate of 87.5%.

The study concludes that fraud is very sensitive and that customers have immense fear of fraud and it impacts negatively on banks profitability where income lost through fraud would have been reinvested to foster growth. Higher profits for a business will indicate that a Bank management is having the right strategy thus sending a positive signal to the market. The study also concludes that the worst fraud risk is identity theft where identification documents are easy to reproduce, fraudsters make parallel passports, IDs and driving licenses then use them to take over accounts. The study further concludes that cheque fraud is a common type of fraud mainly because customers with cheque books are not careful in ensuring that their books are kept in safe custody. The Bank’s IT infrastructure is designed to support the monitoring process by producing daily reports and alerts to be actioned. The study also revealed that a whistle blowing facility is existent in the Bank.
The study recommends that there should be reforms in the police. This could help reduce the fraud related risks in the bank. The recommends that since the judiciary is a key player in Fraud Management and that over the time, it has been seen that courts often acquit or hand in lenient sentences to deadly fraudsters, the judiciary needs to be empowered through reform to be able to understand and be of help. The study also recommends that review of Fraud Legislation could reduce fraud related risks in the banks. Kenya still lags behind on anti fraud laws. The study also recommends that review of security features of security documents (The Kenyan National ID, Driving licenses, passports and Title deeds) would also eliminate fraud related risks in the bank. Other recommendations suggested include staff Management where staff need constant monitoring and motivation of staffs. Appropriate methods should be put in place to deal with the situations. Methods such as employee screening, staff account monitoring, profiling of staff disciplinary cases, job rotation and enrichment are worth considering.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>DECLARATION</td>
<td>ii</td>
</tr>
<tr>
<td>DEDICATION</td>
<td>iii</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td>v</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td>ix</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td>x</td>
</tr>
<tr>
<td>LIST OF ABBREVIATIONS/ACCRONYMS</td>
<td>xi</td>
</tr>
<tr>
<td>CHAPTER ONE: INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>1.1 Background of the Study</td>
<td>1</td>
</tr>
<tr>
<td>1.1.1 Strategic Response</td>
<td>2</td>
</tr>
<tr>
<td>1.1.2 Fraud Related Risks</td>
<td>2</td>
</tr>
<tr>
<td>1.1.3 Commercial Banking Industry in Kenya</td>
<td>3</td>
</tr>
<tr>
<td>1.1.4 Equity Bank Kenya Limited</td>
<td>4</td>
</tr>
<tr>
<td>1.2 Research problem</td>
<td>5</td>
</tr>
<tr>
<td>1.3 Objectives of the Study</td>
<td>6</td>
</tr>
<tr>
<td>The objective of this study was to:</td>
<td>6</td>
</tr>
<tr>
<td>1.4 Value of the study</td>
<td>6</td>
</tr>
<tr>
<td>CHAPTER TWO: LITERATURE REVIEW</td>
<td>8</td>
</tr>
<tr>
<td>2.1 Introduction</td>
<td>8</td>
</tr>
<tr>
<td>2.2 Response Strategies</td>
<td>8</td>
</tr>
<tr>
<td>2.2.1 Fraud Detection Response Strategies</td>
<td>9</td>
</tr>
<tr>
<td>2.2.2 Fraud Investigation Response Strategies</td>
<td>11</td>
</tr>
<tr>
<td>2.2.3 Fraud Prevention Response Strategies</td>
<td>12</td>
</tr>
<tr>
<td>2.2.4 Fraud Control Response Strategies</td>
<td>14</td>
</tr>
<tr>
<td>2.3 Fraud Related Risks in Banks</td>
<td>15</td>
</tr>
<tr>
<td>CHAPTER THREE: RESEARCH METHODOLOGY</td>
<td>17</td>
</tr>
<tr>
<td>3.1 Introduction</td>
<td>17</td>
</tr>
<tr>
<td>3.2 Research Design</td>
<td>17</td>
</tr>
<tr>
<td>3.3 Data Collection</td>
<td>17</td>
</tr>
<tr>
<td>3.4 Data Analysis</td>
<td>18</td>
</tr>
</tbody>
</table>
CHAPTER FOUR: DATA ANALYSIS, RESULTS AND DISCUSSION ............................................. 19

4.1 Introduction ...................................................................................................................... 19

4.2 General Information ........................................................................................................ 19
    4.2.1 Gender of the Interviewees ...................................................................................... 19
    4.2.2 Age of the Interviewees ........................................................................................... 19
    4.2.3 Name of Department ............................................................................................... 19
    4.2.4 Interviewees’ Designation ....................................................................................... 20
    4.2.5 Length of Duration in the Company ........................................................................ 20

4.3 Findings of the study ....................................................................................................... 20
    4.3.1 Fraud Related Risks ............................................................................................... 20
    4.3.2 Strategic Intervention to Manage Fraud-Related Risks ............................................ 23

4.4 Discussions ...................................................................................................................... 29

CHAPTER FIVE: SUMMARY OF THE FINDINGS, CONCLUSIONS AND RECOMMENDATIONS ................................................................................................................................. 31

5.1 Introduction ...................................................................................................................... 31

5.2 Summary of the Findings ............................................................................................... 31

5.3 Conclusions ...................................................................................................................... 33

5.4 Recommendations .......................................................................................................... 35

5.5 Recommendations for Further Studies .......................................................................... 36

5.6 Recommendations for Policy and Practice .................................................................... 37

REFERENCES .......................................................................................................................... 38

APPENDICES ........................................................................................................................... 40

Appendix I: Interview Guide ................................................................................................. 40
LIST OF TABLES

Table 4.1: Response Rate.........................................................Error! Bookmark not defined.
Table 4.2: Gender of the Interviewees........................................Error! Bookmark not defined.
Table 4.3: Age of the Interviewees..............................................Error! Bookmark not defined.
LIST OF FIGURES

Figure 4.1: Response Rate ...............................................................Error! Bookmark not defined.

Figure 4.2: Gender of the Interviewees........................................Error! Bookmark not defined.

Figure 4.3: Age of the Interviewees..............................................Error! Bookmark not defined.
# LIST OF ABBREVIATIONS/ACCRONYMS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACEF</td>
<td>Association of Certified Fraud Examiners</td>
</tr>
<tr>
<td>AICPA</td>
<td>American Institute of Certified Public Accountants</td>
</tr>
<tr>
<td>ATM</td>
<td>Automated Teller Machine</td>
</tr>
<tr>
<td>BCCI</td>
<td>Bank of Credit and Commerce International</td>
</tr>
<tr>
<td>CEO</td>
<td>Chief Executive Officer</td>
</tr>
<tr>
<td>CPA</td>
<td>Certified Public Accountants</td>
</tr>
<tr>
<td>HR</td>
<td>Human Resource</td>
</tr>
<tr>
<td>IFA</td>
<td>International Federation of Accountants</td>
</tr>
<tr>
<td>SAS</td>
<td>Statement on Auditing Standards</td>
</tr>
</tbody>
</table>
CHAPTER ONE: INTRODUCTION

1.1 Background of the Study

Strategy refers to the machinery of the resources and activities of an organization to the environment in which it operates (Johnson and Scholes 2002). Strategic responses as the set of decisions and actions that result in the formalization and implementation of plans designed to achieve a firm’s objectives (Pearce and Robinson (1997). It is through strategic management that a firm will be able to position and relate itself to the environment to ensure its continued success and also secure itself from surprises brought about by the changing environment (Ansoff and McDonnell (1990). He further argues that this can be done by firstly, positioning of the firm through strategy and capability planning in its rightful competitiveness, and secondly, use of real time response through issue management and thirdly, systematic management of resistance during strategic implementation strategic responses are concerned with decisions and actions meant to achieve business objectives and purpose, it answers the question on where does an organization want to go, where it is now and how to get MNGF to where it wants to go (Denis, Lamothe and Langley, 2001).

In 1998, Burnes asserted that the concern in real time responses is to minimize the sum to total losses and restore profitability to ensure organization’s success in a turbulent and surprising environment. By planning, an organization is able to identify the problems and plan how to solve them by using appropriate strategies. Financial fraud is a situation in which the legal and ethical management of financial resources does not take place. In most countries around the world, this type of fraud occurs due to deliberate decisions and actions made by people who handle money and other assets on behalf of employers or clients in a banking institution. However, there are a few places around the world where the unintentional mishandling of funds is also classified as fraud and is subject to the same legal censure as any deliberate action (Hill and Jones (2001)
1.1.1 Strategic Response

Strategic responses are concerned with decisions and actions meant to achieve business objectives and purpose. Strategy answers the fundamental questions of ‘where do we want to go?; Where are we now?; and how do we get there?’ Three areas of a company strategy are important in identifying the responses of a firm to its environmental challenges. These include: Objective setting which involve long term and short term goals; the vision and mission of the company; Strategic directions which involve what business activities should the company concentrate in and where; Competitive strategy where after considerations of the firm’s competitive strengths and weaknesses vies-a-vi competition and customer needs, the company establishes a position of competitive advantage, (Lowes 1994).

The cognitive approach has been used to detect fraud by utilizing information about an auditor’s expectations regarding the likelihood that fraud has occurred, and his/her degree of perceptual field dependence. The same approach has also been used to detect fraud by enabling the auditor to think like the fraud perpetrator and thus avoid being fooled by the culprit’s deception tactics. According to Johnson et al.’s cognitive model, while management attempts to deceive the auditor by utilizing both their knowledge of the business and accounting practices as well as deep cognitive strategies and tactics (e.g. masking, double play, mimicking, dazzling, inventing, repackaging, decoying) and constructing a deception, auditors can use strategies and tactics (e.g anti-mimicking) for detecting such deceptions (Bernardi, 1994). The present author maintains that the usefulness of the various fraud detection approaches mentioned will be enhanced if they are used to supplement one another. If auditors, however, are going to detect fraud they ought to know about the etiology of fraud, i.e why fraud is committed and by whom.

1.1.2 Fraud Related Risks

Fraud is defined by the Malaysian Approved Standards on Auditing (2001), AI No. 240, as an intentional act by one or more individuals among management, employees, or third parties, which results in a misrepresentation of financial statements. Concise English dictionary defines fraud as an act of deceit, scam, con, cheat, hoax, scandal by means of false representation to obtain an unjust advantage. Fraud is believed to be amongst the most serious corporate problems, and challenges in today's business environment, indeed Palshikar (2002) suggests that fraud or scam is a dominant white collar crime in today's business environment … many businesses and
government organisations, particularly in financial and related services, suffer from fraud of various kinds. In the banking industry, many frauds are perpetrated through falsified payment instruments. Common fraud types include; Cheque fraud, computer fraud, Card fraud and Mail order fraud that’s commonly referred to as internet fraud.

The phenomenon is empirically supported by a number of studies; for example, Cain (1999) and the KPMG Australia fraud survey (KPMG, 2002) each indicate that over 50 per cent of all interviewees surveyed believed that fraud is a major business problem. Similarly, reviews of fraud cases by Rezaee (2004) revealed that financial statement fraud has cost market participants more than $500 billion during recent years, with serious litigation consequences for associated auditors. Fraud can be perpetrated on organisation both from outside – the external threat – and from within. Organisations can be set up for the principal purpose of defrauding others and, using the agency of a limited company; fraudsters can perpetrate serious economic offences shielding themselves behind the veil of incorporation. Fraud is now the crime of choice of organized criminal gangs worldwide. The likely gains are enormous and the likelihood of apprehension and thus of conviction and punishment comparatively small compared with conventional crimes of dishonesty involving guns, intimidation and violence of all kinds. Professional criminals are targeting big business.

1.1.3 Commercial Banking Industry in Kenya

The Companies Act, the Banking Act, the Central Bank of Kenya Act and the various prudential guidelines issued by the Central Bank of Kenya (CBK), govern the Banking industry in Kenya. The banking sector was liberalised 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. The CBK publishes information on Kenya’s commercial banks and non-banking financial institutions, interest rates and other publications and guidelines. Banks in Kenya have come together under the Kenya Bankers Association (KBA), which serves as a lobby for the banks’ interests and addresses issues affecting its members.

There are forty-six banks and non-bank financial institutions, fifteen micro finance institutions and forty-eight foreign exchange bureaus in Kenya. Thirty-five of the banks, most of which are
small to medium sized, are locally owned. The industry is dominated by a few large banks most of which are foreign-owned and yet some partially locally owned. Six of the major banks are listed on the Nairobi Stock Exchange. The commercial banks and non-banking financial institutions offer corporate and retail banking services but a small number, mainly comprising the larger banks, offer other services including investment banking.

1.1.4 Equity Bank Kenya Limited

The Equity bank which was established in 1984 as building society has since grown and eventually transformed into a banking corporation. Equity bank has grown to be the dominant bank institution in Kenya. It has its network spanning all over in the country with 123 branches and 43 branches in Uganda, and 3 in Southern Sudan. Equity Bank is the leading inclusive bank in Africa, listed at the Nairobi and Uganda Stock Exchanges. It is the largest bank in the region in terms of customer base with over 5.7 million bank accounts, and 57% of all bank accounts in Kenya. Its presence in Uganda & Southern Sudan is growing. The vision of Equity Bank Ltd is to champion the social economic prosperity of the people of Africa while its purpose is to transform the lives and livelihoods of people socially and economically by availing them modern, inclusive financial services that maximize their opportunities. The multi-currency, multi-company, multi-country system has a capacity of 35 million accounts and a processing speed of 300,000 transactions per minute.

Equity Bank has received both local and global accolades for its unique and transformational financial model. The bank is credited for taking banking services to the people through its accessible, affordable and flexible service provision. At the Africa Investor Index Series Awards 2009 held at the New York Stock Exchange. Equity Bank was named the best performing company in Africa while the Bank’s CEO; Dr James Mwangi was named Africa’s CEO of the year, in the Africa 100 CEO category Index.

In June 2009 Equity Bank was the emerging markets most sustainable bank of the year in Africa and the Middle East. Equity is the holder of the 2007 Global Vision Award in Microfinance "for initiating a concept of the future that will shape the Global Economy". The world renowned Super brands has recognized Equity as the only banking Super brand in East Africa in its first Super brand edition for East Africa in 2008. Equity Bank enjoys an A+ Credit rating from Global
Credit Rating Agency. Equity Bank offers financial services through its wide network of Branches in Kenya, Uganda and Sudan supported by Alternate Delivery Channels. These Channels include: Visa branded ATM’s in Kenya; Points of Sale (POS) where customers shop pay and withdraw cash in leading retail outlets; Internet and mobile banking channels. The Bank runs on a Global Robust State of the Art Information Technology Computer System supported by Infosys, HP, Oracle and Microsoft.

1.2 Research problem

Banking sector has been losing a lot of money through fraudulent activities of which have an impact in their profitability. There is therefore need to curb fraud especially due to emergence of terrorism, Polatoglu et al (2001). In the Kenyan situation, in the 1980s specifically 1986 saw a couple of banks lose a lot of money. The collapse of Rural Urban credit and bank of credit and commerce (BCCI) and the banking crisis that followed in the 90s were all to blame on the abuse of the banking code, by those entrusted on safeguarding customer’s deposits, while trying to get to the bottom of the scams there were a lot of limitations to the success of curbing the escalating fraud. It is in this view that this project seeks to define the causes and ways of minimizing fraud.

Crime in Kenyan banks has evolved from simple crimes of petty theft and forgeries to hi-tech computer based cyber crimes. Fraud has manifested itself in various ways for example; Forgery which is an act of commission by an individual that result in falsification of document with intent to cause deception or purported fraud. It is an act of making a copy or an imitation of something in order to deceive people. Frauds in Kenyan banks only prove that financial liberalization aggravates the inherent tendency of shallow markets to foster excessive speculation and worsens the systematic consequence of such speculative activity. Revelations of fraud, evidence of insider trading and consequent collapse of investor interest have led to an almost unstoppable downturn in Kenyan banks. Bank frauds concern all citizens. It has become a big business today for fraudsters.

These bodies include national Commission on Fraudulent Financial Reporting (Treadway Commission, 1987), AICPA Expectation Gap Roundtable (AICPA, 1992), public Oversight Board of the AICPA’s SEC Practice Section (AICPA, 1993), commission to Study the Public’s Expectations of Audits (Macdonald Commission, 1988), financial Reporting Commission (Ryan

Local studies that have been conducted include Cheptumo,(2010) who tried to establish response strategies to fraud related challenges by Barclays bank of kenya. Wanamba(2010), conducted study on strategies applied by commercial banks in kenya to combat fraud. Bisamaza (1999) who carried a study towards a model to solve problems of congestion in commercial banks in Kenya, Ghebrecristo (2000), who carried out a study on training methods and techniques in an organization: a case study of the Commercial Bank of Africa ltd. Nairobi, Kenya and Okutoyi (1999) who conducted a research on the relationship between the use of strategic marketing and bank performance in Kenya just to mention a few. Therefore, to the researcher's knowledge, at the time of the study, no local or international studies had ever focused on response strategies to fraud related challenges adopted by Equity Bank in Kenya to counter increasing fraud risks. This is despite the ever increasing cases of fraud risks that had claimed a number of financial institutions in Kenya and thus calling for strategic responses to curb the spread of the crime. It is in this light that the researcher aims to fill the existing knowledge gap by carrying out an investigation into the response strategies to fraud related risks with reference to Equity bank of Kenya. The study seeks to answer the question: what are the response strategies to fraud related risks adopted by Kenyan banks with specific reference to Equity bank of Kenya?

1.3 Objectives of the Study

The objective of this study was to:

i. Establish the strategic response to fraud related risks by Equity bank of Kenya Limited

ii. Identify the fraud related risks faced by Equity Bank of Kenya Limited

1.4 Value of the study

The study would be important not only to Equity bank managers but also other managers in the banking sector and to larger extent managers of other industries. It would help them understand the strategic practices and how its understanding can help different firms reduce or curb fraud related risks in their organizations and employ internal control systems. The study would also
help other managers know the methods used in gathering and applying various strategic practices, which would help them improve their management styles.

The results of this study would also be invaluable to researchers and scholars, as it would form a basis for further research. The students and academics would use this study as a basis for discussions on fraud risks and the strategic responses. The study would be a source of reference material for future researchers on other related topics; it would also help other academicians who undertake the same topic in their studies.
CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

This chapter presents a review of the related literature on the subject under study presented by various researchers, scholars, analysts and authors. The materials are drawn from several sources which are closely related to the theme and the objective of the study.

2.2 Response Strategies

Strategic response is the reaction of a firm or an organisation to environmental changes/turbulence i.e. machinery of the resources and activities of an organization to the environment in which it operates. They can be viewed as the matching of activities of an organisation to the environment in which it operates. When firms are faced with unfamiliar changes they should revise their strategies to match the turbulence (Ansoff and MC Donnel, 1990). Strategic responses affect the long-term direction of an organisation and require commitments and resources both human and financial. According to Pearce and Robinson (1991) strategic responses is the set of decisions and actions that result in the formulation and implementation of plans designed to achieve a firm’s objective. It is thus a reaction to what is happening in the environment of the organisation.

According to Pearce and Robinson (2005) it is through strategic responses that a firm is able to position and relate itself to the environment to ensure its continued success and also secure itself from surprises brought about by the changing environment. Strategic responses adopted by companies reflect the firm’s internal strengths and the opportunities faced in the external environment. Strategy will also consider how best to deal with internal weakness and avoid external threats. Hill and Jones (2001) note that internal new venturing is a strategy employed when a company has a set of valuable competencies in its existing business that can be leveraged to enter a new business area. Science based companies use their technology to create market opportunities in related areas mainly through internal new venturing. A firm can also use this strategy to enter and compete in a new business area or an emerging market where there are no established players.
2.2.1 Fraud Detection Response Strategies

A number of approaches to the assessment of fraud risk have been put forward in an attempt to enhance fraud detection by auditors. Some Arthur (1995) has suggested the use of pre-emptive fraud investigation which is a review intended to assess the vulnerability of an organization to fraud. According to Sadgrove (1996) for such a review to be carried out successfully, one needs (a) to have adequate knowledge about both how fraud happens as well as about fraud indicators, and (b) to undertake a fraud vulnerability analysis of the company concerned. A vulnerability analysis assesses: what assets might be at risk; who might take them and who might benefit; how they might take them and sell them and, finally, how effective the controls are. Others Sorensen (1980) have proposed the use by auditors of the triangle model which comprises: (a) a strong, involved, investigative board of directors; (b) a sound, comprehensive system of internal controls; and (c) alert, capable independent auditors. The same authors also pointed out that if any of the points in the triangle do not function properly, the entire triangle will collapse, and the opportunity for management fraud is increased.

One of the most common ways to detect computer fraud is to log exceptions and to follow up on unusual activities in the logs. Exceptions that should be investigated include, for example: Transactions that are out of sequence, out of priority or otherwise out-of-standard; Aborted runs and entries, including repeated unsuccessful attempts to enter the system; Attempts to access applications or functions beyond a person's authorization level. If problems are uncovered, access logs and web activity logs may provide vital clues for tracking down the person involved. Some organizations implement logging, but only on a limited basis. Data may be refreshed or overwritten too frequently for the logs to be useful for gathering evidence at alter date. Logs should be maintained for at least a few months before being erased. Newly developed intrusion detection systems use artificial intelligence capabilities to detect unusual transactions flowing through a system. These are evolving and have the potential of providing an order-of-magnitude improvement in crime detection technology.

Other authors have proposed more specific methods for determining if fraud has occurred and is concealed in the financial statement. The widely-known red flags approach involves the use of a checklist of fraud indicators. The following examples of red flags are listed by Sadgrove: less
physical stock in the warehouse than is shown by computer records; an employee suddenly gaining a lot of wealth, allegedly from an inheritance or a pools win and so forth; an employee who never takes a holiday; a supplier being given an undue amount of work or whose additional costs are accepted or who receives multiple orders at below the threshold for tendering unexplained credit notes; accounts that do not generate an invoice but are used for samples or guarantee claims.

It needs to be remembered, however, that red flags do not indicate the presence of fraud but represent conditions associated with fraud; in other words, they are cues meant to alert an auditor to the possibility of fraudulent activity, Porter (1993) which could have a material impact on the financial statement in a given circumstance. The use of red flags is recommended in textbooks on fraud detection and in auditing standards. The use of red flags questionnaires has three main advantages as a result of which one could reasonably expect them to increase the possibility of detecting fraud, namely raising the auditor’s sensitivity to the possibility of fraud, adding structure to the consideration of fraud, and providing consistency among auditors. A number of authors, however, have cast doubt on the predictive utility of red flags in fraud detection since they are plagued by two limitations: (a) while red flags are associated with fraud, the association is not perfect, and (b) since they focus attention on specific cues they might well inhibit the auditor from identifying or observing other reasons (Pinkus 1989).

According to Johnson et al (1993) the cognitive approach concerns itself with auditors’ thinking and reasoning that underlies their fraud-detection decision making. The cognitive approach has been used to detect fraud by utilizing information about an auditor’s expectations regarding the likelihood that fraud has occurred, and his/her degree of perceptual field dependence. The same approach has also been used to detect fraud by enabling the auditor to think like the fraud perpetrator and thus avoid being fooled by the culprit’s deception tactics. According to Johnson et al.’s cognitive model, while management attempts to deceive the auditor by utilizing both their knowledge of the business and accounting practices as well as deep cognitive strategies and tactics (e.g. masking, double play, mimicking, dazzling, inventing, repackaging, decoying) and constructing a deception, auditors can use strategies and tactics (e.g anti-mimicking) for detecting such deceptions (Bernardi, 1994).
2.2.2 Fraud Investigation Response Strategies.

Investigation consists of performing extended procedures necessary to determine whether fraud, as suggested by the indicators, has occurred. It includes gathering sufficient evidential matter about the specific details of a discovered fraud. All computer fraud investigations need to start with a plan for gathering and handling the evidence. Internal auditors, lawyers, investigators, security personnel, and other specialists from inside or outside the organizations are the parties that usually conduct or participate in fraud investigations. The investigator must be familiar with good systems administration practices and possess extensive background of skills and knowledge relevant to computer security and various concepts at work in the areas under investigation (Wright, 2000). When fraud has been detected, an organization’s main concern is to identify the source of fraud and to determine whether it is an internal or an external problem.

When a fraud investigation reveals irregularities, which may have an adverse impact on the financial position and results of operations, the internal auditors should inform the appropriate management and the audit committee. A suspect should not be confronted until supporting evidence has been gathered. Confrontation should be done by persons who specialize in investigating criminal activity, not by internal auditors. Investigating a case may involve covert operations, surveillance, informants, dumpster diving and sources of information (Apostolou, 2000c).

When fraud has been detected, an organization’s main concern is to identify the source of fraud and to determine whether it is an internal or an external problem. According to the IIA Standards (SIAS No. 3), the roles of internal auditing in the investigation of fraud include: assessing the probable level and extent of the complexity of fraud within the organization; assessing the qualifications and the skills of the internal auditors and the specialists available to participate in the investigation to ensure that it is conducted by individuals having the appropriate type and level of technical expertise to effectively carry out the investigation; being cognizant of the rights of alleged perpetrators and personnel within the scope of the investigation and the reputation of the organization itself; designing procedures to follow in attempting to identify the perpetrators, extent of fraud, techniques used, and cause of fraud; and coordinating activities with management personnel, legal counsel, and other specialists as appropriate throughout the course
of the investigation. When a fraud investigation reveals irregularities, which may have an adverse impact on the financial position and results of operations, the internal auditors should inform the appropriate management and the audit committee. A suspect should not be confronted until supporting evidence has been gathered. Confrontation should be done by persons who specialize in investigating criminal activity, not by internal auditors.

Investigating a case may involve covert operations, surveillance, informants, dumpster diving and sources of information (Apostolou, 2000a). Covert (undercover) operations may be used to prove the allegation of fraud. The court deems the undercover operations, as an acceptable method of acquiring information, provided there is sufficient probable cause that a crime has been committed. Surveillance is the secretive and continuous observance of a suspect's activities and is frequently used in developing evidence. It may be used to obtain probable cause for search warrants, develop investigative leads, identify co-conspirators, gather intelligence, and locate persons or objects. Informants are persons who have specific knowledge of a criminal activity. Informants can be extremely useful in fraud investigations regardless of their personal motivation for supplying information.

Dumpster diving is used when the investigator finds it necessary to sift a suspect's trash to obtain evidence and leads. Important documents and information concerning illegal activity may be found in garbage. The courts have upheld that investigators may sift through trash without a search warrant, provided that the trash has left a suspect's possession. After it has left the suspect's possession, there is no longer the reasonable expectation of privacy, and thus it is a fair game.

### 2.2.3 Fraud Prevention Response Strategies

The Accounting officer is ultimately held accountable for the design and implementation of a fraud prevention strategy and plan. It must further be emphasized that an understanding of overall risk (cumulative effect of inherent, control and detection risk) in relation to fraud risk is critical to the success of a fraud prevention plan. The value of internal control is apparent in both preventing and detecting fraud as prevention is better than cure. A weak internal control creates opportunities for fraud and about half of all frauds occur in the financial area (Vanasco, 1998). Internal control system has four broad objectives; those are to safeguard assets of the firm; to
ensure the accuracy and reliability of accounting records and information; to promote efficiency in the firm's operation; and to measure compliance with management's prescribed policies and procedures (Havey, 1999). The effectiveness of internal control depends largely on management integrity.

The management of every organization must be proactive in preventing fraud from occurring. A review may identify the areas of risk, and a policy may outline the right way to act, but it will all come to naught without preventative action. Some actions to consider include: Background verification of job candidates prior to employment; Due diligence on prospective vendors, suppliers, and/or business partners; Demand controls to avoid unnecessary over-ordering of inventory and consumables and clear purchasing authorization levels; Close monitoring of controls in identified high-risk areas, which in many organizations will include purchasing, payroll, expenses and treasury.

Fraud prevention is the responsibility of every employee, vendor, supplier, contractor, service provider, consultant or any other agency(ies) doing business / having business relationship with the Company to ensure that there is no fraudulent action being indulged in, in their own area of activity/responsibility. As soon as they learn of any fraud or have suspicion regarding it, they should immediately report the matter as per the procedure laid down in the memorandum of association. According to Thomas 2004, all Departmental Heads should be responsible for prevention & detection of fraud and for the proper 'implementation of the Fraud Prevention Policy of the company. He further states that The company should recognize that employee/stakeholders awareness is essential for the effective detection/prevention of fraud/suspected fraud. As such the company shall put in place adequate communication mechanisms for dissemination of information about the policy and its importance to the corruption free governance of the company.

Vanasco (1998) emphasized that fraudulent financial statements were a great concern to the corporate world and the accounting profession. In particular, the author examined the roles of professional associations, governmental agencies and international accounting and auditing bodies in promulgating standards to deter and detect fraud in the US and a few other countries. Vanasco also examined the impact of management and employee fraud on various business
sectors, government bodies and non-profit entities. He discussed the roles of management, the board of directors, the audit committees, auditors, and fraud examiners as well as their liabilities in fraud prevention and investigation. The author explained the ideal control environment to prevent fraud and also focused on the techniques and preventive procedures in the investigative and reporting process. In addition, the writer elaborated on white-collar crimes constituting employee fraud, embezzlement, kiting, larceny, lapping and pilferage. Vanasco also noted several accounts in the financial statements that are vulnerable to fraud. The limitation of the paper is that it did not focus on the impact of fraud on accounting transactions and financial statements. It failed to measure the effect of fraud to victims in monetary terms and the psychological impact on the morale of the employees.

2.2.4 Fraud Control Response Strategies

Fraud control procedures should have three realistic and measurable goals: Reduce losses resulting from fraud; Deter fraud through proactive policies; and Increase the likelihood of early fraud detection. Fraud control policies should provide guidelines on ways to reduce the risk of fraud. For example, a comprehensive security program assists in the prevention and detection of computer fraud from all sources. The use of various layers of properly implemented protection mechanisms will have the synergistic effect of increasing and enhancing a security program. Currently, many experts considered the “onion” model of security as the best and safest approach to manage the risks dealing with computer fraud (KPMG, 2001).

In each instance where fraud is detected, Line Management should reassess the adequacy of the current internal control environment (particularly those controls directly impacting on the fraud incident) to consider the need for improvements. The responsibility for ensuring that the internal control environment is reassessed and for ensuring that the recommendations arising out of this assessment are implemented and lie with Line Management of the division concerned (Trevino and Victor, 2008).

Internal audit provides an independent and objective review and advisory service to: provide assurance to the CEO / Board that the financial and operational controls designed to manage the entity’s risks and achieve the entity’s objectives are operating in an efficient, effective and ethical manner; and assist management in improving the entity’s business performance. Internal
audit can specifically assist an entity to manage fraud control by providing advice on the risk of fraud, advising on the design or adequacy of internal controls to minimise the risk of fraud occurring, and by assisting management to develop fraud prevention and monitoring strategies. An effective internal audit plan should include a review of those fraud controls designed to address the significant fraud risks faced by an entity.

Many entities choose to outsource various aspects of their fraud control arrangements. The Fraud Control Guidelines provide information on the outsourcing of fraud control activities, the key criterion being that the outsourcing does not compromise the entity’s fraud control arrangements. In reaching the decision to outsource aspects of its fraud control arrangements, an entity must ensure the outsourced provider is: suitably qualified and experienced; complies with the requirements of the Fraud Control Guidelines; is familiar with the entity’s internal policies and procedures and applicable legislative responsibilities, as well as any potential conflicts of interest; and committed to complying with the requirements of the Privacy Act 1988.

In addition, it is better practice for an entity outsourcing any or all of its fraud control to ensure:
A fraud risk assessment is undertaken as part of the development or update of its existing fraud control plan; The fraud control plan covers all aspects of the entity, including its programs and services; An in-house contact point is assigned for reporting and recording all allegations of fraud; and the purchasing entity appoints a manager to be responsible for fraud control overall. While all or part of the fraud control arrangements can be outsourced, entities remain accountable for meeting their obligations under legislated requirements and the Fraud Control Guidelines.

2.3 Fraud Related Risks in Banks

Fraud can be defined as an act that involves the use of deception to obtain an illegal advantage. Crime in Kenyan banks has evolved from simple crimes of petty theft and forgeries to hi-tech computer based cyber crimes. Fraud has manifested itself in various ways for example; Forgery which is an act of commission by an individual that result in falsification of document with intent to cause deception or purported fraud.
In most cases, the fraudulent handling of financial resources will lead to substantial losses for an investor or a corporation. The financial loss is sometimes carefully hidden in the accounting records that are used to track activity involving the resources, allowing it to continue until a great deal of money and other assets are siphoned off and no longer in the control of the owner. Business fraud of this type may be conducted by any company officer or employee who has access to corporate resources, and may continue for an extended length of time before becoming apparent. There are several different ways that financial fraud can take place. The most common approach is to misappropriate funds or other resources. For example, submitting an expense report containing line items for legitimate expenses that never took place could be considered fraudulent activity. Falsifying financial statements and records would also be considered an example of financial fraud. Accounts Receivables and Payables are deliberately altered to hide the fact that funds taken in by the company are diverted for the personal use of someone involved in the accounting process. In some cases, two sets of accounting records may be maintained. One set is a true and accurate accounting, while the other is the altered accounting that can be used to divert suspicion of illegal activity when and as necessary.

Frauds in Kenyan banks only prove that financial liberalization aggravates the inherent tendency of shallow markets to foster excessive speculation and worsens the systematic consequence of such speculative activity. Revelations of fraud, evidence of insider trading and consequent collapse of investor interest have led to an almost unstoppable downturn in Kenyan banks. Bank frauds concern all citizens. It has become a big business today for fraudsters. Failure to prevent and detect fraud has serious consequences for organizations. Although rare in occurrence, financial statement fraud can result in devastating losses to investors, creditors and auditors. Detecting fraud is a difficult task for auditors, in part because most have never experienced fraud in their careers (Montgomery et al., 2002).
CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This chapter is a blueprint of the methodology that was used by the researcher to find answers to the research questions. In this chapter the research methodology was presented in the following order, research design, target population, sampling procedure, and data collection methods, instruments of data collection, the data analysis and finally the ethical issues that was considered during the study.

3.2 Research Design

This was a case study since the unit of analysis is one organization. This was a case study aimed at getting detailed information regarding Equity Bank of Kenya response strategies to fraud related risks. According to Yin (1994) a case study allows an investigation to retain the holistic and meaningful characteristics of real life events. Kothari, (2004) noted that a case study involves a careful and complete observation of a social unit. It is a method of study in depth rather than breadth and places more emphasis on the full analysis of a limited number of events or conditions and other interrelations. Primarily data collected from such a study is more reliable and up to date.

3.3 Data Collection

The researcher used both primary and secondary data. Primary data was collected using self-administered interview guides while secondary data was collected by use of desk search techniques from published reports and other documents. Secondary data sources include the company’s publications, periodicals and information obtained from the internet.

The interview guide had open-ended questions. The open-ended questions enabled the researcher to collect qualitative data. This was used in order to gain a better understanding and possibly enable a better and more insightful interpretation of the results from the study. The interview guide designed in this study comprised of two sections. The first part included the demographic. The second part was devoted to the identification of fraud related risk facing Equity bank limited.
The third part sought to establish response strategies to fraud related risks by Equity bank was put into focus. The interview guide was administered to the head of security department, head of finance department and head of operations through one on one interview method to give the respondent time to respond to the questions at their convenience.

3.4 Data Analysis

A content analysis was employed. Content analysis was used to analyze the respondents’ views about the response strategies to fraud related challenges by Equity bank of Kenya. The data was then coded to enable the responses to be grouped into various categories. Tables and other graphical presentations as appropriate were used to present the data collected for ease of understanding and analysis.
CHAPTER FOUR

DATA ANALYSIS, RESULTS AND DISCUSSION

4.1 Introduction
This chapter presents analysis and findings of the study as set out in the research methodology. The study findings are presented on to establish the strategic response to fraud related risks by Equity bank of Kenya Limited and identify the fraud related risks faced by Equity Bank Limited. The data was gathered exclusively from the questionnaire as the research instrument. The questionnaire was designed in line with the objectives of the study.

4.2 General Information

4.2.1 Gender of the Interviewees
On gender composition, the study found that 60% of the interviewees were male, while 40% of the interviewees consisted of female. These findings imply that the bank employs both male and female staff where the male staffs in the management level are slightly more than the female staff.

4.2.2 Age of the Interviewees
The interviewees were required to indicate the age brackets under which their ages fell. 40% of the interviewees were aged between 41 – 50 years, 35% of the interviewees were aged 51 years and above, while 25% of the interviewees were aged between 41 – 50 years. None of the interviewees was aged below 30 years.

4.2.3 Name of Department
The study sought to know the departments from which the interviewees were drawn from. Form the responses, the interviewees were from risk management, security department, sales and marketing, corporate banking, public relations, credit department, sales, finance, customer care department, and information technology departments.
4.2.4 Interviewees’ Designation

The interviewees that responded to the research instruments held various designations in the bank such as risk manager, operations manager, sales clerk, bank clerk, public relations officer, credit officer, finance officer, customer care officer, and IT assistant.

4.2.5 Length of Duration in the Company

On the length of time the interviewees had worked in the company, majority of the interviewees indicated that they had worked in the company for a period between 7 and 10 years, while a small number of the interviewees had worked in the company for a period of 4 to 6 years and an even smaller number of the interviewees had worked in the company for more than 10 years.

4.3 Findings of the study

4.3.1 Fraud Related Risks

The study sought to investigate how sensitive the issue of fraud was to the customers of this bank. All the interviewees of the study indicated that fraud is very sensitive and that customers have immense fear of fraud. This shows that fraud is highly sensitive issue in the Equity bank as well as other banks.

The study further sought to investigate the effect fraud risk have on the competitiveness of the banking institutions. Majority of the interviewees indicated that fraud impacts negatively on banks profitability where income lost through fraud would have been reinvested to foster growth. Higher profits for a business will indicate that a Bank management is having the right strategy thus sending a positive signal to the market. This signal will have a convincing effect on investors and will also put the company on a better position to compete. On the other hand, rampant incidences of fraud in an institution will certainly impact on the company’s reputation. The signaling effect is that the company is about to collapse. In the current era where information is fast, no person would want to be associated with a rotten institution. In terms of competition, the affected firm will not only face mass exodus of clients but will also have loss of loyalty. The firm will not compete favorably-where the interviewees cited the example of G4S limited.
The interviewees were also required to indicate the worst form of fraud in the Bank. The interviewees indicated that the worst fraud risk was identity theft where they said that in modern day society, identification documents are easy to reproduce, fraudsters make parallel passports, IDs and driving licenses then use them to take over accounts.

On the contribution of technology to the banks fraud levels, the interviewees indicated that technology has opened up operations in the banks to global connectivity, the banks are now branchless as all of them are wired together therefore a customer can go to any branch to carry out a transaction. This makes customer identification more difficult. Transaction processing times that was taking longer now take shorter times leaving little time for more keen checks. While technology increased turn around times, it has also been used by fraudsters to commit frauds. Bank operations such as online transactions, swifts, transfers and other payments operate on technology platforms and customer data is also stored electronically. Therefore unauthorized access to sensitive bank information may cause great losses. It’s more challenging because changes in technology are also unpredictable and technology levels also change.

The study required the interviewees to identify the weak areas that expose the bank to fraud in the bank. The study found that information technology management is weak that exposes the bank to fraud in terms of access levels, audit trail and system changes. Other weak areas include internal frauds which involve collusion with fraudsters, plastics credit and debit card frauds and transactions which include forgery of cheques, forged instructions and consumer (Loan) frauds.

The study sought to investigate the capacity and functionality of fraud investigation strategies adopted by Equity Bank in response to fraud risks. The interviewees indicated that fraud management in the Bank is anchored on 5 key departments which include Compliance, Risk and Advisory services (RAS), Control and Governance(C&G), Equity Internal Audit (BIA) and Barclay’s Security and Investigations Services & Fraud Management (BSIS & FM). All the departments work jointly as a team towards eradicating fraud. The Compliance department deals with issues of account opening screening, due diligence on vendors and AML. The also implement group sanctions. RAS is charged with carrying out risk tests on all new products that are to be introduced into the market. They carry out assessments on new and existing products to identify any loop holes that fraudsters can use to siphon money out. They ensure that sufficient
controls are in place for new products to be rolled out. They also carry out continuous checks for existing products in the market to ensure that they updated in line with any changes in the operating environment. BIA is the internal Audit function of the Bank. Its role is to check whether requisite procedures are in place and are followed. Control & Governance department is a retail function that takes care of all control issues in the retail outlets (branches). The department is structured into regions headed by Senior Control Managers and their work is to ensure that control procedures are followed. BSIS & FM is a head office department. Its core function is advice on security matters, offer fraud training and carry out investigations. All cases are reported into the department for action. The department reports directly into the COO to insulate it from unnecessary influence. The team is charged with enforcing the Group Fraud Policy. It makes recommendation to the Group Chief Executive of Financial Crimes who is based in Equity PLC, UK through the Country COO.

The interviewees of the study were requested to comment on the occurrence of the various fraud types in the Bank. They indicated that cheque fraud is common. This is mainly because customers with cheque books are not careful in ensuring that their books are kept in safe custody. The interviewees also indicated that forgery is another common fraud. This occurs where customer signatures on payments instruments such as cheques, cards, and transfer orders may be forged. It was also indicated that Card Fraud (Plastic) in EQUITY is also common type of fraud since EQUITY is an Issuing and Acquiring bank. The Bank issues debit and credit cards to customers. It also acquires merchants who accept both local and International card payments by customers and its behalf. EQUITY processes payments on VISA, MasterCard and AMEX cards. Card Fraud is the most common area of Fraud in the Bank.

The study identified 4 fraud types in the card business; such as Stolen/Lost card:- Fraudsters take possession of lost card and present it to obtain goods at a merchant establishment, Counterfeit card which is a parallel card reproduced from a genuine customer’s card through processes known as skimming. 80% of the card frauds are due to counterfeiting. These are card not present transactions (CNP):- A fraudster obtains card details from a customer’s card and uses it to make online transactions like purchasing airline tickets. Details commonly needed for online card transactions (ecommerce) are the Card no., name of customer, expiry date and a number known as the CVV2. For this fraud type to succeed, fraudsters have to recruit merchant staffs to extract
the details from unsuspecting customers who are settling their bills using the cards. This is a very common type of Fraud in the Card business. The other type is NRI (Not received as issued):-In this scenario, Fraudsters intercept cards on mail. This fraud is not very common but it happens. Transfers fraud is done through identity theft, fraudsters may obtain a genuine customers account details and use them fraudulently to generate false instruction to banks to transfer funds to their preferred destinations. Although the fraud is not common, it tends to cause more losses because as it often targets big accounts. Staff Fraud:-Staff fraud in EQUITY is not very common because there is an embedded fraud culture on staff. Sufficient controls to mitigate staff fraud such as audit trails are in place. Staffs are also well trained and avenues to identify possible suspects are elaborate. There are also strict guidelines and penalties of dealing with culprits. This therefore makes fraud by staff unattractive.

4.3.2 Strategic Intervention to Manage Fraud-Related Risks

The study sought to investigate whether the bank has a fraud policy in place. The interviewees indicated that there is a Group Fraud Policy that’s applicable to all Equity Banks in the world. The policy is maintained by the Group Financial Crime Risk CEO in UK.

Upon indicating that the bank has a fraud policy in place, the interviewees were required to highlight briefly the employed style /model of strategy implementation at bank. The study found that the group policy defines Fraud in its entirety and sets out the strategic direction, priorities and objectives for managing fraud risk. The policy sets out the blueprint for fraud control requirements, fraud risk assessments according to respective Business units and also lays out the general fraud control strategy providing fraud targets that units need to observe. The policy is structured into business units for ease of implementation and gives the escalation process.

The study further required the interviewees to comment on the Bank’s fraud strategy with respect to the various aspects. With respect to authenticity of account opening documents, the interviewees indicated that opening of new accounts is the most robust process. The documents are verified at the point of entry (the branch or a Sales centre) by two designated Bank officials. Verification is done through checking the copies against the originals. The documents are then forwarded to another department known as OPC for further processing. At this stage, the account opening documents are further checked. The Bank also carries out a random check christened
“the Eye-ball”. This is a random selection of account opening documents by a dedicated team of Fraud Samplers. The team picks a sample at random and carries a thorough end to end authentication. When the process is satisfactory, the details of the applicant are forwarded to CRB for customer historical data. The entire process is lengthened because it’s considered to be the critical point of entry by customers into the Banks network.

With regard to pre-employee screening, the interviewees said that this is an HR function. New employees have to be screened to ensure that only those candidates with clean records are taken on board. Applicants are required to submit certificates of good conduct obtained from the Director of CID. For those employees who have worked with other institutions within the Banking industry, recommendations from their former employers are sought. The Bank will also talk to the former employer directly to verify any information required. Otherwise all applicants for employment in Equity have to submit at least three referees who must be reachable at short notice. On Fraud Awareness on the anti Fraud culture, the interviewees indicated that Equity Bank of Kenya is a member of the Equity group. The group code of conduct and Ethics sets out the standards to be embraced by all staff. It’s mandatory for new employees to the Bank to go through induction training on Fraud Management. They will also sign attestations that they have been trained and will strive in their employment to make the Banks premises free from Fraud. The same is enforced by the Head of Security and Investigation (BASIS). Fraud awareness is also a continuous exercise through refresher courses and also through Fraud Alerts.

On the transactions monitoring, the interviewees indicated that transactions in the Bank are screened for normalcy and for anti money laundering (AML). The Bank’s IT infrastructure is designed to support the monitoring process by producing daily reports and alerts upon transactions by customer. The business sets out parameters to be used for monitoring and the parameters are reviewed consistently to be in tune with the Market. Transactions that are not in sync with customer operating range will be picked as red flags and will be looked into by relevant arms of the Bank.

The interviewees also indicated that credit and debit card transactions are monitored by a team of Fraud Analysts who operate 24hrs. Their role is to check for any unusual transactions on customers accounts. For any irregularities, the customer is contacted to verify a transaction.
When a customer declines a transaction, the Fraud Analyst will caution the card to avoid further usage. An incident will also be raised at this stage for the matter to be investigated. This applies to usage of banking instruments such as cheques and transfer instructions (SWIFT, EFTs and RTGSs). Any abnormal usage or eye catching transactions detected on a customer’s account that are not in synch with a customers behavior, the bank will call the customer to verify the transactions. Some transactions that may fall on the AML radar are investigated and may be reported as suspicious transactions reports (STR’s) to CBK for further action under the prudential guidelines. Corporate and Premier Customers have fully dedicated relationship managers who keep an eye on their accounts on a regular basis and alert the customers for any suspicious transactions.

On the reporting processes of detected cases, it was found that the Head of Equity Security and Investigations & Fraud Management (BSIS & FM) is mandated to investigate all reported cases and make recommendations to the business executive committee on action to be taken. All business units within the country have 24hrs to report cases detected to the Head of BSIS & FM. The business units will be required to raise an incident report and sent it to the attention of the Head of BSIS & FM. For sensitive cases that use of normal escalation channels is believed to prejudicial, the bank has provided a whistle blowing facility. This will take care of cases that may involve officers of different ranks in the bank to avoid victimization. Whistle blow lines are maintained by the Head of BSIS & FM and only him can retrieve information. The whistle blow facility allows a reportee / informer to make a report while remaining anonymous. Other than the internal channels, the Bank has also created a contact centre to receive complaints, reports and information from customers and disseminate the same to various relative centers for action. The Contact centre was set up in 2008 and is open 24hrs. The centre is mandated to also follow up the queries to the right departments to ensure that action has been done and appropriate communication has been provided to the customer. The department is based at the Banks main operations centre at Bishops Gate along Bishops rd, in Nairobi

With regard to dispensations to open accounts, the interviewees indicated that there are no dispensations to open accounts. The bank operates a strict account opening policy and all customers have to meet the requirements to open accounts. The same is also monitored by central Bank for compliance. As a measure of gravity of the process, Equity Bank have created
an independent unit to deal with account opening. The unit is known as KYC and main function is to receive account opening requests from Branches and verify them in detail for compliance with the group standards. They also liaise with other institutions of the Bank such as HR, BSIS&FM and Compliance to make sure that customers taken on board into the Bank’s systems are good. KYC also works with other departments outside the Bank such as CRB, Principal Immigrations office and the principal registrar of persons to ensure that documentations provided to open accounts are valid.

The study also revealed that a whistle blowing facility is existent in the Bank. The facility sits with the Head of BSIS &FM who downloads information from the receiving facility and allocates it for investigations. Reports that are sensitive an anonymity is desirable are reported through the facility. This is a very effective facility especially for checking high level internal frauds. The facility is free and available to all employees across ranks. Information is treated with utmost confidence and the whistle blowing line is displayed conspicuously on all Equity centers for all to see and make good use.

With respect to online transactions (opening of new accounts, deposits, transfers, balance inquiries), the interviewees indicated that opening of accounts is an elaborate process which begins when a customer walks into a branch to open an account. The first encounter will be face to face where a Bank staff will receive customer documents and certify with the originals. The remaining process will be back office work and will not require the customer’s presence. Automation of the account opening process is not applicable in the Bank. Further, the Bank recently introduced a system known as “Hello Money” where customers can bank from the comfort of their rooms or offices. Customers can deposit money or inquire for balances in their accounts. To enlist into the facility, the customer needs to satisfy certain conditions which include good banking record in the bank. A customer enjoying the product must be able to keep secret codes such as PIN numbers off head to avoid compromise of card data. Customers under the category will sign indemnities to assure the bank that they will take due care of the bank codes and will solely use them for official use. To transact in the Hello money program, a customer will be issued with a secret PIN. The customer will be required to destroy the PIN after memorizing and henceforth apply the PIN on all the transactions. The Bank will verify the
transactions when the customers PIN matches with the corresponding PIN in the Bank. This also applies to cash deposits on the ATMs.

The study further sought to identify the procedures in place to ensure that an employee doesn't award or manage a transaction where he or she has a financial interest in the vendor providing the product or services. The interviewees indicated that the bank operates on a “maker-checker” authorization process. A person posting a transaction will not authorize that transaction. It will be authorized by a person of a higher level for dual control. For tenders, the Bank has certain predetermined group of vendors who have been authorized to deal with the Bank. The vendors are selected after going through a due diligence process where their background is checked, their financial capability and integrity scales. The tendering committee will only recommend the choice of a vendor but will not make a final decision to award a tender. The final decision will rest with the Executive committee of the Bank chaired by the Chief Finance Officer (CFO). The segregation of function will make impossible for any interested person at any level to sway the process for his personal gain.

The interviewees were required to indicate whether they believe the Bank recognizes the role played by staff in the fight against fraud. The interviewees indicated that the bank greatly appreciates the role played by members of staff in frustrating frauds.

On indicating that they believe that the Bank recognizes the role played by staff in the fight against fraud, the interviewees were required to state how they are recognized. Majority of the interviewees indicated that in line with the fraud culture, any staffs who manage to stop a fraud that would have culminated into a loss will receive mementos that range from certificates of recognition, gifts, promotions and even increased bonuses. This recognition will go into their files and one will be eligible to even promotions when opportunities arise. The Bank values good conduct and any demonstration of the same will be rewarded. Many types of awards such as the COO’s ward, the Chairman’s award are up for winning. The bank carries out on yearly basis an employee opinion survey (EOS) and the result as been favorable.

The study requested the interviewees to give recommendations on what could be done to reduce the incidences of Fraud in the Bank. The interviewees indicated that reforms in the police could
help reduce the fraud related risks in the bank. They indicated that the police are charged with the responsibility of investigating and apprehending criminals. Frauds are perpetrated by criminals. It’s the work of the Police to carry out thorough investigations in order to punish criminals, penetrate into the underworld of fraudsters and frustrate their efforts. When police fall back on this cardinal role or investigate poorly, Kenya can only become a destination of choice for fraudsters.

The interviewees also indicated that to reduce the fraud related risks in the bank there is need to relook at the judiciary. The interviewees argued that since the judiciary is a key player in Fraud Management and that over the time, it has been seen that courts often acquit or hand in lenient sentences to deadly fraudsters, the judiciary needs to be empowered through reform to be able to understand and be of help. The magistrates need to be exposed to international practices in developed countries where frauds have even driven banks to closure so that they understand the gravity of the problem. Those countries have now put in place strict laws to manage fraud; the result is that criminals in those countries are now running into countries like Kenya.

The interviewees also indicated that review of Fraud Legislation could reduce fraud related risks in the banks. Kenya still lags behind on anti fraud laws. The Anti-money laundering act was just passed the other day while others have not been passed. The Card industry in the country faces a real risk from fraudsters because supporting laws have not been enacted. The communications act and the rules of evidence in the country have to be reviewed to be in sync with the current challenges. Bank operations are now hi-tech on technology. The crimes have also spontaneously gone hi-tech therefore calling for amendments to the laws. For example, a person involved in ecommerce may engage in an electronic transaction with a client in Japan. The two partners will not meet face to face and there will be no binding executions to be made. When Fraud occurs, the Kenyan businessman will suffer. The situation will be worse if the instruction is hacked by a fraudster in between.

From the findings, it was also clear that review of security features of security documents (The Kenyan National ID, Driving licenses, passports and Title deeds) would also eliminate fraud related risks in the bank. The documents are main instruments that are recognized in the Banking industry in Kenya. The ID, Passport and Driving license is required to open accounts and to
transact on the accounts; the title deed is collateral to obtain credit. The documents are now
easily counterfeited and banks are exposed to greater risks. Kenya is becoming a destination of
criminals. The Nigerians, Bulgarians and Russians are flooding the market due to its ease in
transit using fake documents. The documents are easily replicated in the streets and fraudulently
used to access money in Banks. It’s possible to have 1000 ID cards in Kenya with different
names. It’s even common for persons to circulate Fake currencies.

Other recommendations suggested include staff Management where human beings need constant
monitoring for it’s said that it’s not weak processes that commit frauds but humans. De-
motivated staffs are bound to commit frauds when they have opportunity to do so. Signs of
disenchanted staff are absenteeism, drunkenness, loneliness, lateness, and irresponsibility.
Appropriate methods should be put in place deal with the situations. Methods such as employee
screening, staff account monitoring, profiling of staff disciplinary cases, job rotation and
enrichment are worth considering. Some functions of monitoring are better performed by
immediate line Managers; others will be performed by HR. The tool to test staff motivation is by
conducting regular structured employee opinion surveys (EOS) to collect employee feelings on a
matter of decision in the Bank as well as system development-as a progress towards fraud
management gains ground owing to its dangers, the Bank must strive to improve its technology
platform to cope with the times. Even with the introduction of the new systems (Flex oracle) that
was launched on the 17/07/2010, continuous development of existing platforms is key- an
institution that is in constant check with itself will always be in ready position for any
environmental changes. Areas such as access rights, audit trails and other upgrades on system
capabilities are paramount.

4.4 Discussions

Fraud is very sensitive and customers have immense fear of fraud and it impacts negatively on
banks profitability where income lost through fraud would have been reinvested to foster growth.
Technology has opened up operations in the banks to global connectivity; the banks are now
branchless as all of them are wired together therefore a customer can go to any branch to carry out a
transaction. This makes customer identification more difficult. Transaction processing times that was
taking longer now take shorter times leaving little time for more keen checks. While technology
increased turn around times, it has also been used by fraudsters to commit frauds. Bank operations such as online transactions, swifts, transfers and other payments operate on technology platforms and customer data is also stored electronically. Information technology management is weak that exposes the bank to fraud in terms of access levels, audit trail and system changes. Cheque fraud is common, mainly because customers with cheque books are not careful in ensuring that their books are kept in safe custody. Forgery is another common fraud. This occurs where customer signatures on payments instruments such as cheques, cards, and transfer orders may be forged. There is a Group Fraud Policy that’s applicable to all Equity Banks in the world. The policy is maintained by the Group Financial Crime Risk CEO in UK which defines Fraud in its entirety and sets out the strategic direction, priorities and objectives for managing fraud risk.

With respect to authenticity of account opening documents, the study established that opening of new accounts is the most robust process. The documents are verified at the point of entry (the branch or a Sales centre) by two designated Bank officials. Transactions in the Bank are screened for normalcy and for anti money laundering (AML). The Bank’s IT infrastructure is designed to support the monitoring process by producing daily reports and alerts to be actioned. The business sets out parameters to be used for monitoring and the parameters are reviewed consistently to be in tune with the Market. Credit and debit card transactions are monitored by a team of Fraud Analysts who operate 24hrs, the Head of Equity Security and Investigations & Fraud Management (BSIS & FM) is mandated to investigate all reported cases and make recommendations to the business executive committee on action to be taken and that there are no dispensations to open accounts. A whistle blowing facility is existent in the Bank. The facility sits with the Head of BSIS & FM who downloads information from the receiving facility and allocates it for investigations. Reports that are sensitive an anonymity is desirable are reported through the facility.
CHAPTER FIVE: SUMMARY OF THE FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter provides the summary of the findings from chapter four, and also it gives the conclusions and recommendations of the study based on the objectives of the study. The objective of this study was to determine the responses by Equity Bank to fraud related risks in the banking industry.

5.2 Summary of the Findings

The study found that fraud is very sensitive and that customers have immense fear of fraud and it impacts negatively on banks profitability where income lost through fraud would have been reinvested to foster growth. Higher profits for a business will indicate that a Bank management is having the right strategy thus sending a positive signal to the market.

The study found that the worst fraud risk was identity theft where they said that in modern day society, identification documents are easy to reproduce, fraudsters make parallel passports, IDs and driving licenses then use them to take over accounts. Technology has opened up operations in the banks to global connectivity; the banks are now branchless as all of them are wired together therefore a customer can go to any branch to carry out a transaction. This makes customer identification more difficult. Transaction processing times that was taking longer now take shorter times leaving little time for more keen checks. While technology increased turn around times, it has also been used by fraudsters to commit frauds. Bank operations such as online transactions, swifts, transfers and other payments operate on technology platforms and customer data is also stored electronically. Information technology management is weak that exposes the bank to fraud in terms of access levels, audit trail and system changes. Other weak areas include internal frauds which involves collusion with fraudsters, plastics credit and debit card frauds and transactions which include forgery of cheques, forged instructions and consumer (Loan) frauds.

The study found that cheque fraud is common, mainly because customers with cheque books are not careful in ensuring that their books are kept in safe custody. The interviewees also indicated
that forgery is another common fraud. This occurs where customer signatures on payments instruments such as cheques, cards, and transfer orders may be forged. It was also indicated that Card Fraud (Plastic) in EQUITY is also common type of fraud since EQUITY is an Issuing and Acquiring bank. The Bank issues debit and credit cards to customers. It also acquires merchants who accept both local and International card payments by customers and its behalf. EQUITY processes payments on VISA, MasterCard and AMEX cards. Card Fraud is the most common area of Fraud in the Bank.

The study found that there is a Group Fraud Policy that’s applicable to all Equity Banks in the world. The policy is maintained by the Group Financial Crime Risk CEO in UK which defines Fraud in its entirety and sets out the strategic direction, priorities and objectives for managing fraud risk. The policy sets out the blueprint for fraud control requirements, fraud risk assessments according to respective Business units and also lays out the general fraud control strategy providing fraud targets that units need to observe. The policy is structured into business units for ease of implementation and gives the escalation process.

With respect to authenticity of account opening documents, the study established that opening of new accounts is the most robust process. The documents are verified at the point of entry (the branch or a Sales centre) by two designated Bank officials. Verification is done through checking the copies against the originals. The documents are then forwarded to another department known as OPC for further processing. When the process is satisfactory, the details of the applicant are forwarded to CRB for customer historical data. The entire process is lengthened because it’s considered to be the critical point of entry by customers into the Banks network.

The study revealed that transactions in the Bank are screened for normalcy and for anti money laundering (AML). The Bank’s IT infrastructure is designed to support the monitoring process by producing daily reports and alerts to be actioned. The business sets out parameters to be used for monitoring and the parameters are reviewed consistently to be in tune with the Market. Transactions that are not in sync with customer operating range will be picked as red flags and will be looked into by relevant arms of the Bank. Further, it was clear that credit and debit card transactions are monitored by a team of Fraud Analysts who operate 24hrs, the Head of Equity Security and Investigations & Fraud Management (BSIS & FM) is mandated to investigate all
reported cases and make recommendations to the business executive committee on action to be taken and that there are no dispensations to open accounts.

The study also revealed that a whistle blowing facility is existent in the Bank. The facility sits with the Head of BSIS &FM who downloads information from the receiving facility and allocates it for investigations. Reports that are sensitive an anonymity is desirable are reported through the facility. Opening of accounts is an elaborate process which begins when a customer walks into a branch to open an account and the bank operates on a “maker-checker” authorization process.

5.3 Conclusions

The study concludes that fraud is very sensitive and that customers have immense fear of fraud and it impacts negatively on banks profitability where income lost through fraud would have been reinvested to foster growth. Higher profits for a business will indicate that a Bank management is having the right strategy thus sending a positive signal to the market.

The study also concludes that the worst fraud risk is identity theft where identification documents are easy to reproduce, fraudsters make parallel passports, IDs and driving licenses then use them to take over accounts. Technology has opened up operations in the banks to global connectivity, the banks are now branchless as all of them are wired together therefore a customer can go to any branch to carry out a transaction. This makes customer identification more difficult. Transaction processing times that was taking longer now take shorter times leaving little time for more keen checks. While technology increased turn around times, it has also been used by fraudsters to commit frauds. Bank operations such as online transactions, swifts, transfers and other payments operate on technology platforms and customer data is also stored electronically. Information technology management is weak that exposes the bank to fraud in terms of access levels, audit trail and system changes. Other weak areas include internal frauds which involve collusion with fraudsters, plastics credit and debit card frauds and transactions which include forgery of cheques, forged instructions and consumer (Loan) frauds.

The study further concludes that cheque fraud is a common type of fraud mainly because customers with cheque books are not careful in ensuring that their books are kept in safe
custody. Forgery is another common fraud which occurs where customer signatures on payments instruments such as cheques, cards, and transfer orders may be forged. It was also indicated that Card Fraud (Plastic) in EQUITY is also common type of fraud since EQUITY is an Issuing and Acquiring bank. The Bank issues debit and credit cards to customers. It also acquires merchants who accept both local and International card payments by customers and its behalf. EQUITY processes payments on VISA, MasterCard and AMEX cards. Card Fraud is the most common area of Fraud in the Bank.

The study deduces that there is a Group Fraud Policy that’s applicable to all Equity Banks in the world. The policy is maintained by the Group Financial Crime Risk CEO in UK which defines Fraud in its entirety and sets out the strategic direction, priorities and objectives for managing fraud risk. The policy sets out the blueprint for fraud control requirements, fraud risk assessments according to respective Business units and also lays out the general fraud control strategy providing fraud targets that units need to observe. The policy is structured into business units for ease of implementation and gives the escalation process.

With respect to authenticity of account opening documents, the study established that opening of new accounts is the most robust process. The documents are verified at the point of entry (the branch or a Sales centre) by two designated Bank officials. Verification is done through checking the copies against the originals. The documents are then forwarded to another department known as OPC for further processing. When the process is satisfactory, the details of the applicant are forwarded to CRB for customer historical data. The entire process is lengthened because it’s considered to be the critical point of entry by customers into the Banks network.

The study also reveals that transactions in the Bank are screened for normalcy and for anti money laundering (AML). The Bank’s IT infrastructure is designed to support the monitoring process by producing daily reports and alerts to be actioned. The business sets out parameters to be used for monitoring and the parameters are reviewed consistently to be in tune with the Market. Transactions that are not in sync with customer operating range will be picked as red flags and will be looked into by relevant arms of the Bank. Further, it was clear that credit and debit card transactions are monitored by a team of Fraud Analysts who operate 24hrs, the Head of Equity Security and Investigations & Fraud Management (BSIS & FM) is mandated to
investigate all reported cases and make recommendations to the business executive committee on action to be taken and that there are no dispensations to open accounts.

The study also revealed that a whistle blowing facility is existent in the Bank. The facility sits with the Head of BSIS &FM who downloads information from the receiving facility and allocates it for investigations. Reports that are sensitive an anonymity is desirable are reported through the facility. Opening of accounts is an elaborate process which begins when a customer walks into a branch to open an account and the bank operates on a “maker-checker” authorization process.

5.4 Recommendations

The study recommends that there should be reforms in the police. This could help reduce the fraud related risks in the bank. The police are charged with the responsibility of investigating and apprehending criminals. Frauds are perpetrated by criminals. It’s the work of the police to carry out thorough investigations in order to punish criminals, penetrate into the underworld of fraudsters and frustrate their efforts. When police fall back on this cardinal role or investigate poorly, Kenya can only become a destination of choice for fraudsters.

The recommends that since the judiciary is a key player in Fraud Management and that over the time, it has been seen that courts often acquit or hand in lenient sentences to deadly fraudsters, the judiciary needs to be empowered through reform to be able to understand and be of help. The magistrates need to be exposed to international practices in developed countries where frauds have even driven banks to closure so that they understand the gravity of the problem. The country should now put in place strict laws to manage fraud. This will reduce fraudsters in the country and hence ensure successful business on the banks in Kenya.

The study also recommends that review of Fraud Legislation could reduce fraud related risks in the banks. Kenya still lags behind on anti fraud laws. The Anti-money laundering act was just passed the other day while others have not been passed. The Card industry in the country faces a real risk from fraudsters because supporting laws have not been enacted. The communications act and the rules of evidence in the country have to be reviewed to be in sync with the current challenges. Bank operations are now hi-tech on technology. The crimes have also spontaneously
gone hi-tech therefore calling for amendments to the laws. The two partners will not meet face to face and there will be no binding executions to be made. When Fraud occurs, the Kenyan businessman will suffer. The situation will be worse if the instruction is hacked by a fraudster in between.

The study also recommends that review of security features of security documents (The Kenyan National ID, Driving licenses, passports and Title deeds) would also eliminate fraud related risks in the bank. The documents are main instruments that are recognized in the Banking industry in Kenya. The ID, Passport and Driving license is required to open accounts and to transact on the accounts; the title deed is collateral to obtain credit. The documents are now easily counterfeited and banks are exposed to greater risks. The documents are easily replicated in the streets and fraudulently used to access money in Banks. Therefore a reform of the security features would ensure reduction of fraud in the banking transactions.

Other recommendations suggested include staff Management where human beings need constant monitoring and motivation of staffs. Appropriate methods should be put in place deal with the situations. Methods such as employee screening, staff account monitoring, profiling of staff disciplinary cases, job rotation and enrichment are worth considering. Some functions of monitoring are better performed by immediate line Managers; others will be performed by HR. Areas such as access rights, audit trails and other upgrades on system capabilities are paramount and should be revisited to ensure the staff does not participate in fraud related transactions.

5.5 Recommendations for Further Studies

This study has explored the strategic responses by Equity Bank to fraud related risks and established that fraud is very sensitive and impacts negatively on banks profitability. The overall effect of fraud can therefore not be ignored at any cost. There is therefore need to respond to these fraud related risks. This study has recommended adoption of various reforms in the bank and in other arms of the government to reduce fraud related risks in the banks in Kenya. The study further recommends that another study needs to be done with an aim of investigating the effectiveness of the strategic responses to fraud related risks in the commercial banks in Kenya.
5.6 Recommendations for Policy and Practice

The study recommends the bank management to come up with a policy which clearly indicates steps to be taken on any staff found committing fraud. This will help reduce internal fraud which is more elaborate in the bank than external.

The study recommends the bank system to be monitored and reviewed to ensure that no gap is left for fraud to be committed without notice. This can be done through employee screening, staff account monitoring, profiling of staff disciplinary cases, job rotation and enrichment.
REFERENCES


Krambia-Kapardis, M. (2002) ‘Fraud victimisation study: Cyprus’ experience’, Ernst and Young, Cyprus; PricewaterhouseCoopers


APPENDICES

Appendix I: Interview Guide

INTERVIEW GUIDE FOR HEAD OF OPERATIONS, FINANCE MANAGER AND HEAD OF SECURITY IN EQUITY BANK OF KENYA

This interview guide consists of two parts; kindly answer all the questions by ticking in the appropriate box or filling in the spaces provided.

PART A: GENERAL INFORMATION

1. What is your Gender?
2. Which is your department?
3. Which is your designation?
4. What is your age?
5. What is your highest level of education?
6. How many years have you worked in this bank?

PART B: RESPONSE OF EQUITY BANK TO FRAUD RELATED RISKS.

1. Which are the various types of fraud risks encountered by Equity bank in its operations?

2. What are the major reasons for people to involve these fraudulent acts Equity bank?
3. How has technology led to increased frauds in the Equity bank?

4. What are the fraud detection strategies adopted by this bank to respond to fraud risks in this bank?

5. What is the capacity and functionality of fraud investigation strategies in the Bank’s response to fraud risks?

6. What are the IT controls for assuring the continuity and rapid recovery of fraud transactions in this bank?

7. How many “transactions” are created in your area using security system?

8. What are the primary controls used to monitor business processed through the bank’s system?
9. How does the department ensure that products and services are charged in accordance with transaction terms?

10. What procedures are in place to ensure that an employee doesn't award or manage a transaction where he or she has a financial interest in the vendor providing the product or services?

11. Who in your department is in charge of monitoring the security of this bank’s systems to prevent fraud?

12. How do the security systems in Equity Bank support the requirements for: administrative controls (e.g., transaction controls, limit controls, accounting controls, etc.); and due diligence assessments?

   a) Administrative Controls

      Transaction controls

      Limit controls
Accounting controls

b) Diligence assessments

13. What would be the best way to improve security or quality for the bank system to prevent fraud?

THANK YOU FOR YOUR TIME AND COOPERATION