RESPONSE STRATEGIES TO FRAUD BY THE LISTED COMMERCIAL BANKS IN KENYA

BY

MBUGUAH CHARLES NJUGUNA

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

OCTOBER 2013
DECLARATION

This research study is my original work and has not been presented for the award of a degree in this University or any other Institution of higher learning for examination.

Signature…………………………….       Date…………………………………….

MBUGUAH CHARLES NJUGUNA

D61/75742/2012

The research project has been submitted for examination with my approval as the University supervisor.

Signature ……………………………….       Date…………………………………….

MR. JEREMIAH KAGWE

LECTURER

DEPARTMENT OF BUSINESS ADMINISTRATION.

SCHOOL OF BUSINESS

UNIVERSITY OF NAIROBI
DEDICATION

This work is dedicated to my family; my wife Jemimah for always being there even when things were tough, my daughter Sarah for her continued challenge and my son Sammy, for his never ending support. Their support, encouragement and dedication have been priceless.
ACKNOWLEDGEMENTS

I acknowledge the power of God, the maker, and the provider of knowledge for enabling me to complete my Masters in the right spirit. I wish to acknowledge the support from my supervisor Jeremiah Kagwe, without whose guidance and support I could not have gone this far with my project work. To the University of Nairobi for offering me the opportunity to do this study and all my lecturers who contributed in one way or another in quenching my thirst for knowledge, I owe you my gratitude.

I cannot forget the positive influence of my classmates as a source of inspiration throughout my study and for assisting me in sourcing for information and materials for this project. To you all, I say may God bless you abundantly.
# TABLE OF CONTENTS

Declaration .......................................................................................................................... ii  
Dedication .......................................................................................................................... iii 
Acknowledgements ............................................................................................................ iv 
List of Figures ................................................................................................................... vii 
List of Tables .................................................................................................................... vii 
Abbreviations and Acronyms ............................................................................................ ix 
Abstract ............................................................................................................................... x 

## CHAPTER ONE: INTRODUCTION ............................................................................. 1  
1.1 Background of the Study .............................................................................................. 1  
1.1.1 Strategic Responses ............................................................................................. 2  
1.1.2 Fraud Management Practices ............................................................................... 3  
1.1.3 The Banking Industry in Kenya ........................................................................... 4  
1.2 Research Problem ......................................................................................................... 5  
1.3 Research Objectives ...................................................................................................... 7  
1.4 Value of the Study ........................................................................................................ 7  

## CHAPTER TWO: LITERATURE REVIEW ................................................................ 9  
2.1 Introduction ................................................................................................................... 9  
2.2 Theoretical Foundation ................................................................................................. 9  
2.3 Concept of Strategy .................................................................................................... 11  
2.4 Response Strategies .................................................................................................... 12  
2.5 Types of Frauds........................................................................................................... 16  

## CHAPTER THREE: RESEARCH METHODOLOGY ............................................. 18  
3.1 Introduction ................................................................................................................... 18  
3.2 Research Design .......................................................................................................... 18  
3.3 Target Population ........................................................................................................ 18  
3.4 Data Collection .......................................................................................................... 19  
3.5 Data Analysis .............................................................................................................. 20  

## CHAPTER FOUR: DATA ANALYSIS, RESULTS AND DISCUSSION .......... 21
4.1 Introduction ................................................................................................................. 21
4.2 Demographic Data ...................................................................................................... 21
4.3 Response strategies to fraud by the listed commercial banks in Kenya ..................... 24
4.4 Discussion of Findings .............................................................................................. 39

CHAPTER FIVE: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS 42
5.1 Introduction ................................................................................................................. 42
5.2 Summary of Findings ............................................................................................... 42
5.3 Conclusions ................................................................................................................ 45
5.4 Recommendations for Policy and Practice ................................................................ 47
5.5 Limitations of the Study ........................................................................................... 48
5.6 Suggestions for further Research ............................................................................. 48

REFERENCES ................................................................................................................ 50

APPENDICES ................................................................................................................. 55
  Appendix I: List of Listed Commercial Banks in Kenya as at 30th September 2013 . 55
  Appendix II: Questionnaire .......................................................................................... 56
LIST OF TABLES

Table 4.1: Name of the respondent’s bank .......................................................... 22

Table 4.2: Respondents working experience .................................................... 23

Table 4.3: Products respondents are familiar with .......................................... 25

Table 4.4: Respondents opinion on the leading causes of fraud in the bank ....... 27

Table 4.5: Respondents known types of fraud ............................................... 28

Table 4.6: The most effective strategy in fighting fraud ................................... 29

Table 4.7: The level of staff involvement in the fraud process ....................... 30

Table 4.8: The major factors contributing to fraud in listed Banks .................. 30

Table 4.9: The Bank’s growth in the last 5 years ........................................... 32

Table 4.10: Effectiveness of fraud address during the growth period .............. 33

Table 4.11: Impartial treatment on staff involved in fraud .............................. 35

Table 4.12: Extent of responding to fraud ...................................................... 36
LIST OF FIGURES

Figure 4.1: Gender of the respondents ................................................................. 22
Figure 4.2: Work Level of the respondents .......................................................... 24
Figure 4.3: Period last trained on these products ................................................. 25
Figure 4.4: Frequency of Fraud training conducted ............................................ 26
Figure 4.5: Level of the bank’s rigorous pre-employment screening ..................... 32
Figure 4.6: Effectiveness of the law enforcement agencies in the fight against fraud .... 33
Figure 4.7: Success of fraud investigations in the respondent banks ................... 34
Figure 4.8: Level of knowledge in fighting fraud in respondent’s current role ........ 37
# ABBREVIATIONS AND ACRONYMS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACFE</td>
<td>Association of Certified Fraud Examiners</td>
</tr>
<tr>
<td>ATMs</td>
<td>Automated Teller Machines</td>
</tr>
<tr>
<td>BFID</td>
<td>Banking Fraud Investigations Department</td>
</tr>
<tr>
<td>CBK</td>
<td>Central Bank of Kenya</td>
</tr>
<tr>
<td>CMA</td>
<td>Capital Markets Authority</td>
</tr>
<tr>
<td>EMV</td>
<td>EuroMastercardVisa</td>
</tr>
<tr>
<td>KYC</td>
<td>Know Your Customer</td>
</tr>
<tr>
<td>NSE</td>
<td>Nairobi Securities Exchange</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification number</td>
</tr>
<tr>
<td>PwC</td>
<td>PricewaterhouseCoopers</td>
</tr>
<tr>
<td>SPSS</td>
<td>Statistical Package for Social Sciences</td>
</tr>
</tbody>
</table>
ABSTRACT

The threat of fraud to banks emanates from both their internal and external environments. Fraud has been and continuous to be a major risk facing banks in Kenya. It is a subject that receives wide coverage in the Kenyan print and electronic media as the figures involved are almost always quite substantial. This study sought to establish the response strategies to fraud by the listed (publicly quoted) commercial banks in Kenya. This study adopted a descriptive survey design because it aimed at giving an accurate description on the response strategies to fraud in the listed commercial banks in Kenya. The target population for this research comprised of all the 11 listed commercial banks in Kenya. The study collected both primary and secondary data using a semi-structured questionnaire while secondary data was obtained from review of reports from the Banking Fraud and Investigations Department of Central Bank and review of periodic reports filed by the listed banks. The study found that the heads of fraud and investigations in listed commercial banks have appropriate experience and knowledge of responding to fraud. The study concluded that the pressures that often motivate fraud are staff frustrations, poor/lack of controls, and lack of product knowledge. The study also found out that preventative, training, detection, prosecution and investigation strategies are used by all the listed banks in managing the fraud menace. The level of staff involvement in the fraud process was found to be reasonably high. Issues around financial over commitment and inadequate reward strategies were noted to be major drivers for staff involvement in fraud. The existence of a whistle blowing policy and fraud policy was found to be very rigorous commensurate with the company’s fraud risk and taking into account applicable legal considerations. All the banks were reported to have gone through various forms of growth in the last 5 years during which time the study found out that fraud was effectively and adequately addressed. The law enforcement agencies play a critical role in fraud management in any jurisdiction. This study concluded that they were moderately successful in the fight against fraud. The fraud investigations by listed commercial banks were found to be successful. The study recommended establishment of units to specialize in proactively targeting and reactively investigating cases of staff fraud, that Banks should invest in technology based fraud fighting tools, enhance the pre-screening of potential employees, train officers on IT investigations as the current fraud trends are through cyberspace, enforce internal controls, emphasizing on know your customer policies and customer due diligence before opening bank accounts. The study recommended a review of the security features on the identification documents used to open accounts as another strategy that could play a great role in frustrating fraud in commercial banks. Another recommendation from this study is for the listed commercial banks to embrace and fast track the adoption of the chip technology in their card business which has been found to be effective. It was recommended that fast tracking of the reforms in the police and judiciary sectors will improve the turnaround of prosecution of cases and sentencing of fraudsters.
CHAPTER ONE: INTRODUCTION

1.1 Background of the Study

Ansoff (1980) noted that the environment is constantly changing, and so it makes it imperative for organizations to continuously adapt their activities to succeed. In order to survive in this very dynamic environment, organizations need strategies to focus on their customers and to deal with the emerging environmental challenges. These environmental changes are more complex to some organizations than others and for survival an organization must maintain a strategic fit with its environment. The environment is important and an organization has to respond to its dynamism, heterogeneity, instability and uncertainty (Thompson, 2005).

The threat of fraud to banks emanates from both their internal and external environments. According to Cressey (1973) for fraud to be successful, three things must be present namely opportunity, pressure and rationalization. Banks must therefore craft effective response strategies to manage the threat posed by fraud. The strategies will invariably require allocation of resources in terms of human, financial etc. yet these resources are scarce and are competed for by various arms of the banks. Without resources, banks would not be able to manage fraud.

Fraud has become a major source of concern for Banks in Kenya. The media is awash with news of how banks are losing billions of shillings every year to fraudsters. While not all fraud losses are reported, figures from the Banking Fraud and Investigations Department
(BFID) of the Central Bank of Kenya indicate that significant amounts are actually lost by banks each year in this country. For listed banks this could lead to a drop in the value of their shares or more stringent oversight/control by their multiple regulators.

1.1.1 Strategic Responses

Ansoff (1965) viewed strategy in terms of market and product choices. According to his view, strategy is the “common thread” among an organization’s activities and the market. Johnson and Scholes (2002) defined strategy as the direction and scope of an organization that ideally matches the results of its changing environment and in particular its markets and customers so as to meet stakeholder expectations. According to Delmar and Shane (2003), strategy is a unified and integrated plan that relates the strategic advantages of the firm to the challenges of the environment and that is designed to ensure that the basic objectives of the enterprise are achieved through proper execution by the organization. Eisenhardt and Martin (2000) perceive strategy as a pattern or a plan that integrates organization’s major goals, policies and action into a cohesive whole. Pearce and Robinson (2001) defined strategy as the company’s “game plan” which results in future oriented plans interacting with the competitive environment to achieve the company’s objectives. Lambert and Knemeyer (2004) stated that managers develop strategies to guide how an organization conducts its business and how it will achieve its objectives. With the changes in the external environment brought about by fast changing technology, changing social and economic landscapes and cut throat competition, organisations must not only scan the environment but must be quick and nimble to respond to these changes.

Faced with an ever increasing threat of fraud which erodes the banks’ profits and customers’ trust in their operations, commercial banks have to make choices on what strategies to adopt
to most effectively manage this menace. In Kenya, we have seen most banks restructuring and upgrading their banking platforms. Majority of the retrenched staff are the long serving experienced people creating a gap in the knowledge of managing fraud. These loopholes have been exploited by fraudsters and could be one of the reasons for the increasing fraud levels. Some of the response strategies taken by the listed commercial banks include the creation of fraud and investigations units, investment in technology e.g. the current migration from magnetic strip cards to chip technology in the plastic card area, creation of avenues for whistle blowing, inclusion of fraud management in the performance contracts of all staff, periodic training and refreshers for all staff etc.

1.1.2 Fraud Management Practices

Various techniques in fraud management have been developed and are used by commercial banks to manage the menace of fraud. Since the fraud management process goes through various stages, the practices are based on the particular stage within what has been referred to by the Journal of Economic Crime Management as the Fraud Management Lifecycle.

According to Dolan (2004) the fraud management lifecycle is made up of eight stages. Deterrence, the first stage, is characterized by actions and activities intended to stop or prevent fraud before it is attempted; that is, to turn aside or discourage even the attempt at fraud through, for example, card activation programs. The second stage of the Fraud Management Lifecycle, prevention, involves actions and activities to prevent fraud from occurring. In detection, the third stage, actions and activities, such as statistical monitoring programs are used to identify and locate fraud prior to, during, and subsequent to the completion of the fraudulent activity.
The intent of detection is to uncover or reveal the presence of fraud or a fraud attempt. The goal of mitigation, stage four, is to stop losses from occurring or continuing to occur and/or to hinder a fraudster from continuing or completing the fraudulent activity, by blocking an account, for example. In the next stage, analysis, losses that occurred despite deterrence, detection, and prevention activities are identified and studied to determine the factors of the loss situation, using methods such as root cause analysis. The sixth stage of the Fraud Management Lifecycle, policy, is characterized by activities to create, evaluate, communicate, and assist in the deployment of policies to reduce the incidence of fraud. Balancing prudent fraud reduction policies with resource constraints and effective management of legitimate customer activity is also part of this stage. An example is the requirement that any cash transaction over $10,000 be reported (Dolan, 2004).

Investigation, the seventh stage, involves obtaining enough evidence and information to stop fraudulent activity, recover assets or obtain restitution, and to provide evidence and support for the successful prosecution and conviction of the fraudster(s). Covert electronic surveillance is a method used in this stage. The final stage, prosecution, is the culmination of all the successes and failures in the Fraud Management Lifecycle. There are failures because the fraud was successful and successes because the fraud was detected, a suspect was identified, apprehended, and charges filed. The prosecution stage includes asset recovery, criminal restitution, and conviction with its attendant deterrent value (Yaukey, 2002).

1.1.3 The Banking Industry in Kenya

Commercial Banking institutions are licensed and regulated pursuant to the provision of the Companies Act, Banking Act, Central Bank of Kenya Act and the Regulations and Prudential Guidelines issued by the CBK from time to time. The current guidelines were issued in
January 2013. Commercial banks are the dominant players in the Kenyan Banking System and closer attention is paid to them while conducting offsite and on-site surveillance to ensure that they operate in compliance with the existing laws and regulations. Currently there are 44 licensed commercial banks and 1 mortgage finance company; out of the 44 institutions, 31 are locally owned and 13 are foreign owned. The locally owned financial institutions comprise 3 banks with significant shareholding by the government and state corporations, 27 commercial banks and 1 mortgage finance institution (CBK Report 2012).

The banking industry in Kenya constitutes private and publicly owned banks. Out of the 44 commercial banks operating in Kenya, 11 are publicly owned and listed in the Nairobi Securities Exchange (NSE). Publicly listed banks in Kenya are the biggest in terms of profits, asset base, number of accounts, distribution channels etc. (CBK Annual Reports). In the last 3 years, the profit before tax of the 11 listed banks which constitute 26% of all licensed banks averaged 74% of the industry totals. They have also suffered some of the highest losses arising from fraud as per the BFIU figures. The banking industry records some of the highest profits in Kenya. Individual banks like Equity Bank, KCB Bank, Barclays Bank and Standard Chartered Bank posted pre-tax profits in excess of kshs10 Billion each in 2012 (CBK Annual Report 2012).

1.2 Research Problem

Strategy is defined by Scholes & Johnson (1993) as the direction and scope of an organization over the long term which achieves advantage for the organization through its configuration of resources within a changing environment, to meet the need of markets and stockholders. Management and other stakeholders of listed commercial banks expect good returns from the banks. Fraud threatens the achievement of this key objective hence the need
to adopt proper strategies to manage or control it. Strategic management is also defined as the set of decisions and actions that results in the formulation and implementation of plans to achieve a company’s objectives (Pearson & Robinson, 2007). Firms have set for themselves strategic objectives in order to acquire and sustain competitive advantage. Efficient management of the fraud menace would give a bank a competitive advantage over others hence the need to adopt strategies that will make this possible and ultimately enable the bank to achieve its objectives.

Ansoff (1980) noted that the environment is constantly changing, and so it makes it imperative for organizations to continuously adapt their activities to succeed. In order to survive in this very dynamic environment, organizations need strategies to focus on their customers and to deal with the emerging environmental challenges. These environmental changes are more complex to some organizations than others and for survival an organization must maintain a strategic fit with its environment. The environment is important and an organization has to respond to its dynamism, heterogeneity, instability and uncertainty (Thompson, 2005). The response strategies of yester year cannot be effective in this highly dynamic environment. Harvey (1993) claimed that computer crime and fraud were more perilous to organizations today. This paper presented the statistics about the growth of fraud, and causes of fraud in the workplace.

Statistics from Banking Fraud and Investigations Department (BFID 2011) show that the frequency of internal fraud is increasing. This is because some dishonest employees and managers have found ways to override systems and/or collude with outsiders to defraud their banks. According to the bank’s fraud unit, management fraud occurs less frequently but
accounts for the greatest financial losses. Position equals power; managers and executives, having more access to more information and assets than regular employees can commit fraud relatively easier without being noticed (Angira, 2011).


My research shows that no study has specifically been carried out on response strategies to fraud by the listed commercial banks in Kenya. This study therefore sought to fill the existing knowledge gap by seeking to answer the following question “What are the Response Strategies to fraud by the listed commercial banks in Kenya?

1.3 Research Objectives

The study sought to establish the response strategies to fraud by the listed commercial banks in Kenya.

1.4 Value of the Study

This study will be beneficial in a number of ways:

It will address the existing knowledge gap in the field of response strategies to fraud by the listed commercial banks in Kenya. It will therefore assist academicians and scholars
interested in the response strategies to fraud in the banking industry as fraud has become a menace to the industry.

The study will assist the listed commercial banks and the wider banking industry in the formulation of strategies, policies, standards, procedures and guidelines that may help in responding to fraud incidences in the banking industry.

It will be used as a resource document for the government and mostly the bank regulator (Central Bank of Kenya) in understanding the different response strategies to fraud management by listed commercial banks and help in the formulation of further policies by the regulator for use in the banking industry.
CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

This section draws on literature in the area of fraud management strategies in the banking industry. Previous studies done in this area are reviewed. It covers the theories on which the study will be based. Various strategies that have been adopted to combat fraud in the banking industry are also reviewed.

2.2 Theoretical Foundation

This study is based on various theories; firstly the theory put forward by Cressey (1973) which came up with the model known as the fraud triangle. The theory posits that for fraud to be successful, three things must be present namely opportunity, pressure and rationalization. The term fraud has been defined in different ways by different authors. According to Boniface (1991) fraud is described as “any premeditated act of criminal deceit, trickery or falsification by a person or group of persons to obtain undue personal monetary advantage.”

Secondly the Resource Based Theory which is a method of analysing and identifying a firm’s strategic advantages based on examining its distinct combination of assets, skills, capabilities and intangibles as an organization. The underlying premise is that firms differ in fundamental ways because each firm possess a unique set of resources, tangible and intangible assets and organizational capabilities to make use of these assets. Each firm develops competencies from these resources and when developed well, these become the source of the firm’s competitive advantages (Pearson & Robinson, 2007). Central to the Resource Based Theory is the definition of three basic types of resources, tangible, intangible and organizational capabilities which become the building blocks for distinctive competencies of a firm (Pearson & Robinson, 2007).
Tangible assets are the physical and financial means a firm uses to provide value to its customers. These are easy to identify and are found in the firm’s balance sheet. Intangible resources are resources such as brand names, patents, trademarks and accumulated experience within a firm. These are assets that cannot be touched but are critical in creating a competitive advantage. Organizational capabilities are the skills, the ability and ways of combining assets, people and processes that a firm uses to transform inputs into outputs. Finely developed capabilities such as customer friendly systems can be a source of sustained competitive advantage, enabling firms to take the same input factors as rivals and converting them into products and services either with greater efficiency in the process or greater quality in the output or both (Pearson & Robinson, 2007). The resources must be critical to being able to meet a customer’s need better than other alternatives, are scarce, drive a key portion of overall profits and are sustainable over time.

Thirdly the Resource Dependency Theory that relates to the need for environmental linkages between the firm and outside resources. A general assumption in resource dependence theory is that the key to organisational survival is the ability to acquire and maintain resources (Pfeffer and Salancik, 1978). In this perspective, directors serve to connect the firm with external factors by co-opting the resources needed to survive. This means that boards of directors are an important mechanism for absorbing critical elements of environmental uncertainty into the firm. Environmental linkages could reduce transaction costs associated with environmental interdependency. The organization’s need to require resources leads to the development of exchange relationships between organizations. Galaskiewicz and Bielefeld (1998) state that the fate of organisations depends upon their access to resources. Further, the uneven distribution of needed resources results in inter-dependent organizational
relationships. Several factors would appear to intensify the character of this dependence, e.g. the importance of the resource(s), the relative shortage of the resource(s) and the extent to which the resource(s) is concentrated in the environment. This theory would be applicable in this study in terms of banks looking at creating a common approach to fighting the menace that faces them in the form of fraud. Secondly fighting fraud requires resources in terms of human, technology, time and finances creating a constraint since resources are scarce.

2.3 Concept of Strategy

Strategy is the direction and scope of the organization over the long term which deliver a competitive edge for the firm amidst an ever changing business environment. Effective strategy configures a firm’s resources and core competencies so as to adequately meet the firm’s goals and objectives. Strategy creates a culture in the firm in which the firm only focuses on the value adding priorities in its mission and vision (Johnson and Scholes, 2008). Competitive strategy is aimed at creating a goodness of fit between the firm’s internal resources capabilities and the environmental challenges faced (Aosa, 1992).

Strategy is a multi-dimensional concept and various authors have defined strategy in different ways. Linn (2008) depicted strategy as the match between an organization’s resources and skills and the environmental opportunities as well as the risks it faces and the purposes it wishes to accomplish. The purpose of strategy is to provide directional cues to the organization that permit it to achieve its objectives while responding to the opportunities and threats in the environment (Pearce and Robinson, 2001).
Johnson and Scholes (2008) defined strategy as the direction and scope of an organization that ideally matches the results of its changing environment and in particular its markets and customers so as to meet stakeholder expectation. According to Delmar and Shane (2003), strategy is a unified and integrated plan that relates the strategic advantages of the firm to the challenges of the environment and that is designed to ensure that the basic objectives of the enterprise are achieved through proper execution by the organization. Eisenhardt and Martin (2000) perceive strategy as a pattern or a plan that integrates organization’s major goals, policies and action into a cohesive whole. Pearce and Robinson (2001) defined strategy as the company’s “game plan” which results in future oriented plans interacting with the competitive environment to achieve the company’s objectives.

2.4 Response Strategies

Strategy refers to a plan of action designed to achieve a particular goal. Strategy is the match between an organization resources and skills and the environmental opportunities it wishes to accomplish. It is important to provide guidance and direction for the activities of the organization. It is the process by which managers set an organization’s long term course, develop plans in the light of internal and external circumstances, and undertake appropriate action to reach those goals. The “Action” referred to here are the strategies employed in meeting a firm’s short and long term objectives (Johnson & Scholes, 2002).

Strategy is about winning. It is a unifying theme that gives coherence and direction to the actions and decisions of an individual or organization. It is not purely a matter of intuition and experience. Analysis does play a role in the strategy process of a company. Strategy guides organizations to superior performance through establishing competitive advantage. It also acts as a vehicle for communication and coordination within organizations. Successful
strategies include objectives that are simple, consistent and long term, good understanding of
the competitive environment, and objective understanding of the resources that is,
understanding strengths and exploiting them and understanding weaknesses and protecting
the organization against them. Understanding the strategic position of an organization and
considering the strategic choices upon to it is of little value unless the managers or
management wish to follow can be turned into organizational action (Johnson & Scholes,
2002).

Strategic responses are the set of decisions and actions in the formulation and
implementation of plans designed to achieve a firm’s objective (Pearce and Robinson, 1991).
They are part of competitive strategies that organizations develop in defining their goals and
policies. They are responses to what is happening in the environment of the Organization.
The general management should be involved in the development of the organization’s
strategic responses. Furthermore for an organization to implement a strategic response, three
components are critical. These are the right climate - will to respond, competence - ability to
respond, and capacity - volume of responses (Ansoff, 1980).

Strategic responses involve changes to the organizational behaviour. Such responses may
take form depending on the organizations capability and the environment in which it
operates. The overall responsibility for the effective responses belongs to the general
management of the firm. Firms can respond to environmental changes by crafting new
operational changes which are taken by functional areas of the organization to achieve
corporate and business unit objectives by maximizing resource productivity. They note that
operational responses are concerned with developing and nurturing a distinctive competence
to provide an organization with a competitive advantage. Operational responses include
Fraud has been classified in various ways and using various parameters; these ways include; management of the banks (otherwise referred to as management fraud); insiders, these perpetrators are purely the employees of the banks; outsiders, these include customers and/or non-customers of the banks; and outsiders/insiders, this is a collaboration of the bank staff and outsiders (Ojo, 2008).

The banking sector in any country plays a fundamental role in increasing the level of economic activity. As intermediaries to both suppliers and users of funds, banks are effectively situated in a continuum that determines the pulse of the economy. Worldwide, the ability or inability of banks to successfully fulfil their role as intermediaries has been a central issue in some of the financial crises that have been witnessed so far. Diamond (1984) posits that a special feature of banking activities is to act as delegated monitors of borrowers on behalf of the ultimate lenders (depositors). In this special relationship with depositors and borrowers, banks need to secure the trust and confidence of their numerous clients. Though this requires safe and sound banking practices, it is not always the case as bank failures in different countries have come to prove.

The failure of banks to adequately fulfil their role arises from the several risks that they are exposed to; many of which are not properly managed. One of such risks which is increasingly becoming a source of worry is, the banking risk associated with fraud.

Fraud, which literally means a conscious and deliberate action by a person or group of persons with the intention of altering the truth or fact for selfish personal gain, is now by far the single most veritable threat to the entire banking industry (Idolor, 2010). Pressure relates to duress that is caused by an employee's perceived immediate need for assets (Cressey,
One group of fraud researchers notes that 95% of all fraud cases involve needs caused by financial difficulties or vice-related activities (Albrecht et al., 1995). In most instances, pressure pushes the fraudster to take significant risks in order to obtain the desired resources. Ironically, a financial emergency need only be perceived in the mind of the perpetrator to lead to the commission of fraudulent acts (Cressey, 1973).

Some of the pressures that often motivate misappropriation of assets include greed or preoccupation with being successful, living beyond one's means, high personal debts, high medical bills, work-related pressures such as low pay, failure to receive a promotion, unfair treatment, lack of respect or dissatisfaction with one's job, boredom ("having nothing else to do") challenge to see if one can "beat the system without getting caught"; and spouse- or family-imposed pressures. This list is not exhaustive but it does identify pressures that fraud researchers have associated with employee fraud (Albrecht et al., 1984; Ratliff et al., 2003; ACFE, 1995).

While internal auditors cannot readily regulate the pressure attribute, they can help mitigate the opportunity to commit fraud. Typical failures in control or control-related issues that increase the opportunity for employee fraud include but not limited to lack of segregation of duties, failure to inform employees about company rules and the consequences of violating them or perpetrating fraud, rapid turnover of employees, constantly operating under crisis conditions, lack of an audit trail, ineffective supervision, lack of transaction authorizations, poor accounting records, lack of physical controls, lack of access to information (by employees other than the ones committing fraud), breakdown of procedures (for example, inappropriate computer access, ineffective physical inventories) (Albrecht et al., 1984; Bologna and Lindquist, 1987).
The third element of the fraud model is rationalization (integrity). Individuals do not commit fraud unless they can justify it as being consistent with their own personal code of ethics (Hollinger and Clark, 1983). For most employees, personal integrity may be the key limiting factor in keeping a person from misappropriating assets. That is, many employees would not perpetrate a fraud even if a need or opportunity arose. Some investigators believe a strong moral code can prevent individuals from using rationalizations to justify illicit behaviour (Hollinger and Clark, 1983; Wells, 1997).

2.5 Types of Frauds

Ziegenfuss (1996) performed a study to determine the amount and type of fraud occurring in state and local government. The study revealed that the most frequently occurring types of fraud are misappropriation of assets, theft, false representation, and false invoices. The reasons for the increased fraud in state and local governments are poor management practice; economic pressure, weakened society values; people being not held responsible for their actions; and inadequate training for those responsible for fraud prevention and detection. Most fraud cases are based on false representations or concealment of materials facts. False representations are those made directly by an interested party to induce action on the part of another, those made by a third party touching some fact which is not the subject of the contract, and those made under such circumstances as to cause unknown persons to act on them (Maguire, 2002).

The most broadly defined of the three types of online banking fraud, identify theft gets the most attention from the media and is the highest concern to consumers. Identity theft can be very simple or quite complex. Identity theft can be extremely difficult for its victims. It can
take months or even years to correct the damage it can cause. If the thief has acquired enough information to satisfactorily answer the questions asked by the financial institution, he or she will be able to use the information to commit fraud. Because the level and types of questions asked can determine whether or not an identity theft succeeds, those questions must be crafted so that only the true person will know the answers (Shannon, 2000).

Online banking has added another channel of internet fraud through which an employee can steal. If a financial institution allows employees access to the customer data, and that data is the same information needed to gain online access to customer accounts, an employee can easily commit fraud. Because of this, financial institutions should require a password or PIN should be stored in an encrypted format, internal fraud through online banking can be the most costly to financial institutions (Omankhanlen, 2009). As financial institutions increasingly offer online banking services to their customers, they must face issues of consumer confidence in the internet. Consumers are concerned about identity theft and wonder if the internet is safe for online banking. The answer is yes, if financial institutions, in co-operation with their customers, make it safe. Therefore building the best controls to prevent fraud and protect customers is of critical importance (Ventura, 2000).
CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This section deals with the methodology used for carrying out the research. It focuses on the research design, target population, research instruments, reliability and validity of instruments, data collection and data analysis.

3.2 Research Design

This study adopted a descriptive survey design. This is because the study aimed at giving an accurate description on the response strategies to fraud in the listed commercial banks in Kenya. A descriptive research is more rigorous than exploratory research and seeks to find out the; who, what, when and how, aspects of the research (Cooper and Schindler, 2006).

This study was a survey research. It was deemed appropriate because the research involved seeking information from persons in banks responsible for responding to fraud incidents in the banks. A cross-sectional study was carried out once and the sample population to make measurements at a specific point in time (Lewis, Saunders and Thornhill, 2011).

3.3 Target Population

Population is the entire group of individuals, events or objects having common characteristics (Mugenda and Mugenda, 2003). According to Cooper and Schindler (2006) population is the total collection of elements about which a researcher wishes to make some inferences. The target population for this research comprised of all the 11 listed commercial banks in Kenya.
The study focused on the listed banks for the following reasons; they contribute 75% of the industry pre-tax profits, they are the largest in terms of asset base, distribution channels etc. They also attract keen interest from the investing public and the various regulatory bodies. The results of the study therefore reflected the sector position.

3.4 Data Collection

The study collected both primary and secondary data. To collect the primary data, a semi-structured questionnaire was used. According to Mugenda and Mugenda (2003) questionnaires are suitable to obtain important information about the population. Orodho (2004) said this method reaches large number of subject who are able to read and write independently.

Primary data was collected by the use of a semi-structured questionnaire. Questions on response strategies in the listed commercial banks in Kenya were used in order to obtain specific information by providing a list of possible alternatives from which the respondents selected the answer that best describes their opinion. Secondary data was obtained from review of reports from the Banking Fraud and Investigations Department (BFID 2012). Review of periodic reports filed by the listed banks was another source of secondary data.

The questionnaire was distributed to the heads of fraud investigations in all the listed commercial banks. The researcher used the drop and pick method as all the banks in scope have their headquarters in Nairobi.
3.5 Data Analysis

Data from the field was edited and coded according to themes which emanated from the research objectives and questions. Descriptive statistical techniques were analysed in data analysis. The coded data was analysed using the statistical package for social sciences (SPSS).

Descriptive statistics such as mean and percentages were utilized to analyse demographic information and the likert type of responses. Responses obtained from the questionnaire were organized, tabulated and analysed through the use of simple frequencies and percentages.
CHAPTER FOUR: DATA ANALYSIS, RESULTS AND DISCUSSION

4.1 Introduction

This chapter contains research findings and discussion of the same. The objective of the study was to establish the response strategies to fraud by the listed commercial banks in Kenya. This study targeted 11 respondents; questionnaires were distributed to all targeted respondents. However, out of 11 questionnaires distributed only 10 respondents fully filled and returned the questionnaires. This constituted a 91% response rate. The study made use of frequency tables and figures to present data. The study targeted heads of fraud investigations in all the listed commercial banks as they are the officials who are involved in the formulation, operationalization and cascade of the response strategies to fraud in their respective banks.

4.2 Demographic Data

The respondents were asked to respond to a series of questions about themselves and the organization.

4.2.1 Name of the respondents bank

The respondents were asked to specify the name of the bank they work for. Table 4.1 gives a summary of the results obtained.
Table 4.1: Name of the respondent’s bank

<table>
<thead>
<tr>
<th>Bank</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Barclays Bank of Kenya</td>
<td>1</td>
<td>10%</td>
</tr>
<tr>
<td>National Bank of Kenya</td>
<td>1</td>
<td>10%</td>
</tr>
<tr>
<td>Housing Finance</td>
<td>1</td>
<td>10%</td>
</tr>
<tr>
<td>NIC bank</td>
<td>1</td>
<td>10%</td>
</tr>
<tr>
<td>Not Indicated</td>
<td>6</td>
<td>60%</td>
</tr>
<tr>
<td>Total</td>
<td>10</td>
<td>100%</td>
</tr>
</tbody>
</table>

**Source: Research Data**

The findings indicate that most 6(60%) of the respondents did not disclose the name of the banks they work for, 1 (10%) indicated they worked for Barclays Bank of Kenya, 1(10%) indicated they worked for National Bank of Kenya, Housing Finance and NIC bank each. Non-disclosure of the bank name could be attributed to the sensitivity of the issue being studied.

### 4.2.2 Gender of the respondents

The respondents were then asked to point out their gender. Below are the results of the findings.

**Figure 4.1: Gender of the respondents**

![Gender of Respondents Chart](chart.png)

**Source: Research Data**
As shown in figure 4.1 above, majority (8) of the respondents were male whereas 2 were female. This implies that more males were tasked with the responsibility of implementing fraud response strategies than their female counterparts. This could be explained by the rigorous and sometimes dangerous nature of the job hence it might not attract ladies.

4.2.3 Working experience

The respondents were required to show the range of no of years they had been working. The results are illustrated in the table below.

**Table 4.2: Respondents working experience**

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-5 yrs</td>
<td>3</td>
</tr>
<tr>
<td>6-15 yrs</td>
<td>4</td>
</tr>
<tr>
<td>over 15 yrs</td>
<td>3</td>
</tr>
<tr>
<td>Total</td>
<td>10</td>
</tr>
</tbody>
</table>

*Source: Research Data*

It is evident from the table that most (4) of the respondents have worked for a period of 6-15 years, 3 of the respondents have either worked for a period of 1-5 years or over 15 years each. This demonstrates that the respondents have the appropriate experience and knowledge of managing fraud.

4.2.4 Work Level of the respondents

The respondents were asked to cite their respective work level. The findings are summarized in figure 4.1 below.
From the findings in figure 4.2 most 5(50%) of the respondents are in senior management level, 4(40%) are in the middle management level while 1(10%) are at the supervisory level. This implies that the respondents are placed at senior levels and can therefore be relied upon to give accurate information on response strategies to fraud by the listed commercial banks in Kenya.

4.3 Response strategies to fraud by the listed commercial banks in Kenya

4.3.1 Products respondents are familiar with

The respondents were given a list of products offered by banks such as credit cards, fixed deposits, mortgage products, savings accounts, current accounts and mobile banking and asked to indicate their familiarity with these products. The study findings are as illustrated below.
Table 4.3: Products respondents are familiar with

<table>
<thead>
<tr>
<th>Product</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit cards</td>
<td>10</td>
</tr>
<tr>
<td>Fixed deposits</td>
<td>10</td>
</tr>
<tr>
<td>Mortgage products</td>
<td>8</td>
</tr>
<tr>
<td>Savings accounts</td>
<td>10</td>
</tr>
<tr>
<td>Current accounts</td>
<td>8</td>
</tr>
<tr>
<td>Mobile banking</td>
<td>10</td>
</tr>
</tbody>
</table>

Source: Research Data

As shown in table 4.3, the respondents were found to be very familiar with credit cards, fixed deposits, savings accounts and mobile banking as depicted by frequency level of 10 each, mortgage products and current accounts followed with frequency levels of 8 each. The findings show that the respondents are very familiar with products and hence able to manage fraud related to these products.

4.3.2 Period last trained on these products

In relation to the above products, the respondents were asked to indicate when they were last trained on them. The study findings are described below.

Figure 4.3: Period last trained on these products

Source: Research Data
Out of the 10 respondents, 70% of them said they had been trained within the last year whereas 30% said they had been trained 1-5 years ago. In order to counter fraud associated with these products, regular training is essential as it increases the personnel know-how. The findings reveal that 70% of the respondents are up to date with the necessary skills required as they were recently trained on them. Continuous training allows for people to be up to date with various product features hence enhancing fraud fighting skills.

4.3.3 Existence of a Bank Whistle Blowing Policy

Asked whether the respondents’ banks have a whistle blowing policy, all the respondents agreed that the banks did. Whistle blowing allows for any member of staff to raise issues on suspect activities and could be both preventative and detective.

4.3.4 Frequency of Fraud training conducted

Fraud training is amongst the strategies in fraud management that have been developed and are used by commercial banks to manage the menace of fraud. The respondents were required to indicate the frequency of fraud training conducted by the banks.

Figure 4.4: Frequency of Fraud training conducted

Source: Research Data
According to figure 4.4 above, majority 7 (70%) of the respondents indicated that fraud training was conducted on a quarterly basis while the remaining 3(30%) of the respondents said it was conducted annually. This depicts that the organisations have sought employee training opportunities in the fraud risks that threaten their business thereby empowering staff to respond to the threat of fraud appropriately.

### 4.3.5 The leading causes of fraud in the bank

The respondents were also asked to give an opinion on the leading causes of fraud in their banks. A summary of the findings are given below.

**Table 4.4: Respondents opinion on the leading causes of fraud in the bank**

<table>
<thead>
<tr>
<th>Cause of Fraud</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of controls within different processes</td>
<td>7</td>
</tr>
<tr>
<td>Staff frustrations</td>
<td>5</td>
</tr>
<tr>
<td>Insufficient procedures</td>
<td>3</td>
</tr>
<tr>
<td>Collusion and compromise of existing controls</td>
<td>3</td>
</tr>
<tr>
<td>Lack of management controls</td>
<td>2</td>
</tr>
<tr>
<td>Lack of product knowledge</td>
<td>2</td>
</tr>
</tbody>
</table>

*Source: Research Data*

From table 4.5 above, lack of controls within different processes had a frequency of 7, staff frustrations followed with a frequency level of 5, insufficient procedures and collusion and compromise of existing controls each had frequency levels of 3 and lack of management controls as well as lack of product knowledge each had frequency level of 2. The findings reveal that lack of control and staff frustrations are major causes of fraud in the listed banks.
4.3.4 Respondents knowledge of types of fraud

The study required the respondents to highlight the types of frauds they have knowledge about. Table 4.6 shows the summary of findings established.

**Table 4.5: Respondents known types of fraud**

<table>
<thead>
<tr>
<th>Type of Fraud</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft and Embezzlement</td>
<td>9</td>
</tr>
<tr>
<td>Defalcation</td>
<td>10</td>
</tr>
<tr>
<td>Forgeries</td>
<td>10</td>
</tr>
<tr>
<td>False Identity</td>
<td>10</td>
</tr>
<tr>
<td>Unofficial Borrowings</td>
<td>9</td>
</tr>
<tr>
<td>Money Laundering</td>
<td>10</td>
</tr>
<tr>
<td>Card Fraud</td>
<td>9</td>
</tr>
<tr>
<td>Computer fraud</td>
<td>10</td>
</tr>
<tr>
<td>Fake payments</td>
<td>10</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>87</strong></td>
</tr>
</tbody>
</table>

Source: Research Data

From the findings, defalcation, forgeries, false identity, money laundering, computer fraud, and fake payments were the most cited frauds by the respondents as depicted by frequency levels of 10 each. Theft and Embezzlement, Unofficial Borrowings, and Card Fraud were also cited with frequency levels of 9 each. This finding portrays that the respondents have knowledge of the major types of fraud experienced in the banking industry and are therefore well placed to respond to the threat of fraud.

4.3.5 The most effective strategy in responding to fraud

The respondents were requested to point out what they consider to be the most effective strategy in responding to fraud.
Table 4.6: The most effective strategy in fighting fraud

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevention</td>
<td>9</td>
</tr>
<tr>
<td>Training</td>
<td>3</td>
</tr>
<tr>
<td>Detection</td>
<td>2</td>
</tr>
<tr>
<td>Prosecution</td>
<td>2</td>
</tr>
<tr>
<td>Investigation</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>17</strong></td>
</tr>
</tbody>
</table>

Source: Research Data

The respondents cited prevention (frequency level of 9) as the most effective strategy, training came in next with a frequency level of 3, detection and prosecution both had frequency levels of 2 and lastly investigation with a frequency level of 1. The findings indicate that preventive strategy and training are proactive and therefore most effective. Detection, prosecution and investigation strategies are reactive therefore less effective in fighting or stopping fraud but they still underscore banks consistent commitment to taking appropriate action when fraud is discovered.

4.3.5.1 Reasons for effectiveness of the mentioned strategy

In relation to the most effective strategy in fighting fraud, the respondents were asked to give reasons for supporting the mentioned strategies.

The respondents held that proactive fraud risk management is better in ensuring that the risk of fraud is detected and frustrated before it happens. Such prevention could be by way of the whistle blowing policy and equipping staff with the necessary skills hence training is rated highly. They also said that training gives birth to prevention as the staff and customers understand various types of frauds in addition to sensitization of personnel on fraud trends. Moreover, the respondents cited investigation and successful prosecution as major deterrent strategies to fighting fraud.
4.3.6 The level of staff involvement in the fraud process

There are numerous types of fraud that can be perpetrated by staff against their employers. Depending on the nature of business and the products and services offered, members of staff may have many opportunities to commit fraud. The respondents were asked to rate the level of staff involvement in the fraud process.

Table 4.7: The level of staff involvement in the fraud process

<table>
<thead>
<tr>
<th>Level</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very high</td>
<td>2</td>
<td>20%</td>
</tr>
<tr>
<td>High</td>
<td>7</td>
<td>70%</td>
</tr>
<tr>
<td>Moderate</td>
<td>1</td>
<td>10%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>10</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

Source: Research Data

The findings reveal that majority 7(70%) of the respondents felt that staff were highly involved in the fraud process, 2 (20%) said staff were very highly involved whereas 1 (10%) reported that staff were moderately involved. This implies that the level of staff involvement in the fraud process on average is high.

4.3.7 The major factors contributing to fraud in listed Banks

The study further sought to investigate the factors contributing to fraud in listed banks. The results are explained below.

Table 4.8: The major factors contributing to fraud in listed Banks

<table>
<thead>
<tr>
<th>Factor</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inadequate staffing</td>
<td>1</td>
</tr>
<tr>
<td>Poor internal controls</td>
<td>6</td>
</tr>
<tr>
<td>Lack of staff training</td>
<td>6</td>
</tr>
<tr>
<td>Financial over commitment</td>
<td>8</td>
</tr>
<tr>
<td>Inadequate reward strategies</td>
<td>4</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>25</strong></td>
</tr>
</tbody>
</table>

Source: Research Data
The respondents highly attributed financial over commitment (frequency level of 8), lack of staff training and poor internal controls each had frequency levels of 6, inadequate reward strategies had a frequency level of 4 while inadequate staffing had a frequency level of 1. This shows that financial over commitment by staff is a major factor followed by poor internal controls which would give opportunity for fraud to be perpetrated.

4.3.8 Frequency of technological systems upgrade

The respondents were also asked to respond on the frequency of technological systems upgrades. All revealed that technological systems upgrade was done as & when it is necessary. This implies that with the changes in the external environment brought about by fast changing technology, the organisations scan the environment and are quick and nimble to respond to these changes.

The same case was identified with regard to the frequency of review of bank’s internal controls and procedures updating.

4.3.9 Level of the bank’s rigorous pre-employment screening

Screening of potential employees involves background checks of criminal history, credit worthiness, verification of previous employment and education documents etc. The respondents were asked to rate their bank’s level of pre-employment screening.
Figure 4.5: Level of the bank’s rigorous pre-employment screening

Source: Research Data

As per figure 4.5, 50% of the respondents said that the bank’s pre-employment screening was very rigorous, 30% said it did not exist, while 10% each said that it was above average and below average as well. The findings depict that an employee screening program should be commensurate with the company’s fraud risk and take into account applicable legal considerations.

4.3.10 The Bank’s growth in the last 5 years

The respondents were requested to point toward their bank’s growth in the last 5 years.

Table 4.9: The Bank’s growth in the last 5 years

<table>
<thead>
<tr>
<th>Segment</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expansion in existing markets</td>
<td>8</td>
</tr>
<tr>
<td>Identification of new market segments</td>
<td>4</td>
</tr>
<tr>
<td>New distribution channels</td>
<td>5</td>
</tr>
<tr>
<td>Total</td>
<td>17</td>
</tr>
</tbody>
</table>

Source: Research Data

According to the findings, expansion in existing markets had a frequency level of 8, new distribution channels had a frequency level of 5, and Identification of new market segments had a frequency of 4. The respondents were further asked how effectively fraud was addressed during this growth period since periods of change can create opportunities
as systems, processes and structures change. The findings are described in the table below.

Table 4.10: Effectiveness of fraud address during the growth period

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effectively addressed</td>
<td>4</td>
<td>40%</td>
</tr>
<tr>
<td>Adequately addressed</td>
<td>4</td>
<td>40%</td>
</tr>
<tr>
<td>Moderately addressed</td>
<td>2</td>
<td>20%</td>
</tr>
<tr>
<td>Total</td>
<td>10</td>
<td>100%</td>
</tr>
</tbody>
</table>

Source: Research Data

Most of the respondents 4 (40%) each said that fraud was effectively and adequately addressed while 2 (20%) said it was moderately addressed.

4.3.11 Effectiveness of the law enforcement agencies in the fight against fraud

Law enforcement agencies and the criminal justice system are a major component in the fight against fraud. Organisations should involve these agencies notably the police at an early stage in the investigation. However this would only happen if they feel that potentially the police will want to prosecute the individuals involved. The respondents were asked to rate the effectiveness of the law enforcement agencies in the fight against fraud. The results are explained in the figure below.

Figure 4.6: The success of the law enforcement agencies in the fight against fraud

Source: Research Data
As shown in the figure, 70% of the respondents said the law enforcement agencies were successful in the fight against fraud, 20% said they were very successful. This could create some apathy in involving the law enforcement agencies which in itself could work for the fraudsters.

4.3.12 Success of fraud investigations in the respondent banks

The figure below illustrates the responses on the Success of fraud investigations in the respondent banks as measured by successful apprehension of the fraudsters.

Figure 4.7: Success of fraud investigations in the respondent banks

Source: Research Data

The findings above show that the respondents rate fraud investigations in their banks as very successful (20%) and 80% of the respondents said that it was successful as measure by the number of successful apprehension of fraudsters. This illustrates that the banks have effective investigation mechanisms in place which translate to high success rates.

4.3.13 Impartial treatment on staff involved in fraud

The study required the respondents to point out whether there was impartial or equal treatment of staff involved in fraud. The table below illustrates the results of the findings.
Table 4.11: Impartial treatment on staff involved in fraud

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>8</td>
<td>80%</td>
</tr>
<tr>
<td>I don't know</td>
<td>2</td>
<td>20%</td>
</tr>
<tr>
<td>Total</td>
<td>10</td>
<td>100%</td>
</tr>
</tbody>
</table>

Source: Research Data

Out of the 10 responses, 8 respondents said that there was impartial treatment of staff involved in fraud, and 2 were not aware of the status of staff treatment. This confirms that the organisations consistently demonstrate their commitment to a zero-tolerance policy with all staff involved in fraud being treated equally.

4.3.14 Top Management concern about fraud prevention/detection

The respondents were asked whether the top management was concerned about fraud prevention/detection (tone at the top). The findings revealed that the respondents unanimously agreed that the top management was extremely concerned about fraud prevention/detection. The tone at the top drives the culture of an organisation.

4.3.15 Extent of combating fraud

The respondents were asked to consider a series of statements on combating fraud and rate the extent to which they apply to their banks. Mean scores and standard deviation were computed for each statement and summarized as in table 4.13.
Table 4.12: Extent of responding to fraud

<table>
<thead>
<tr>
<th>Strategy to respond to fraud</th>
<th>Mean</th>
<th>Std. Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application of Know Your Customer as a strategy to respond to fraud</td>
<td>4.9000</td>
<td>.31623</td>
</tr>
<tr>
<td>Pre-screening of new staff as a strategy to respond to fraud</td>
<td>4.3000</td>
<td>1.25167</td>
</tr>
<tr>
<td>Periodic fraud training to employees as a strategy to respond to fraud</td>
<td>4.2000</td>
<td>.78881</td>
</tr>
<tr>
<td>Regular auditing of transactions by internal and external auditors as a strategy to respond to fraud</td>
<td>4.2000</td>
<td>78881</td>
</tr>
<tr>
<td>Adoption of new technology as a strategy to respond to fraud</td>
<td>3.9000</td>
<td>.87560</td>
</tr>
<tr>
<td>Whistle blowing facility as a strategy to respond to fraud</td>
<td>4.4000</td>
<td>.51640</td>
</tr>
<tr>
<td>Application of strong internal controls facility as a strategy to respond to fraud</td>
<td>4.4000</td>
<td>.84327</td>
</tr>
</tbody>
</table>

Source: Research Data

As shown in the table, most of the respondents agreed that the application of Know the Customer as a strategy to respond to fraud was applied a mean score of 4.9; moreover they agreed that the banks have a whistle blowing facility with a mean score of 4.4; additionally they agreed that the application of strong internal controls with as a strategy to respond to fraud rating a mean score of 4.4. Also the respondents agreed that pre-screening of new staff as a strategy to respond to fraud mean score of 4.3; they also agreed that there was periodic fraud training to employees on strategies to combat fraud, as well as regular auditing of transactions by internal and external auditors strategies to combat fraud with a mean score of 4.2. Finally, the respondents agreed that the adoption of new technology strategies to combat fraud with a mean score 3.9. These findings demonstrate that various response strategies to fraud have been adopted by the listed commercial banks in Kenya.

4.3.16 Level of knowledge in fighting fraud in respondent’s current role

The respondents were also asked to rate their level of knowledge in fighting fraud in their current roles. The findings are presented below.
As illustrated in figure 4.7 above, majority (70%) of the respondents held that they were very highly knowledgeable in fighting fraud, 20% held that they were highly knowledgeable and 10% held that they were moderately knowledgeable.

In relation to knowledge in fighting fraud, the respondents were asked whether fraud management formed part of their performance Contract/ responsibility to fight/manage fraud. All the respondents agreed that their performance was measured on their ability to fight fraud/manage fraud. These findings show that the organisations were properly equipped in terms of employee know how to fight fraud and had placed responsibility and accountability with the right people.

4.3.17 Person responsible for preventing fraud in the Bank

The study in addition sought to establish the respondents’ opinion on the persons responsible for preventing fraud in the Bank. It came out clearly that they all were of the
opinion that all members of staff were responsible for preventing fraud and everyone had a role to play.

4.3.18 Existence and enforcement of Bank Fraud Policy

Establishing written policies and procedures, and assigning responsibility for implementing them, for follow up and/or investigation when “red flags” are noted, policy and procedure violations occur, and allegations of improprieties surface is critical to ensure that investigation and remediation occurs. Asked about the existence and enforcement of a fraud Policy, majority (9) of the respondents agreed that it was in existence and enforceable while one respondent did not know of this. These findings portray that a fraud policy is in pace and is enforced in majority of the listed banks.

4.3.19 Recommendation on fraud reduction

The respondents were finally asked to make recommendations for the banks to help reduce level of fraud. The recommendations given include; Banks should invest in driven fraud management tools, ensure thorough screening of new employees; routinely train officers on IT investigations to give them skills as the current trends show a shift towards internet banking-electronic frauds; enforce internal controls; emphasizing on KYC and customer due diligence before opening bank accounts and adoption of new technology of EMV-chip cards. They also recommend the fast tracking of judiciary reforms to ensure prosecution of offenders and turnaround time of determination of cases is shortened. Another recommendation was the creation and maintenance of a databank for known fraudsters and the sharing of such data between the banks.
4.4 Discussion of Findings

The study ascertained that the respondents’ banks have a whistle blowing policy. Similarly, the Institute of Directors of Southern Africa (2002) encourages boards of directors to consider the need for a confidential reporting process (“whistle-blowing”) covering fraud and corruption. The study also found that the pressures that often motivate fraud are staff frustrations, poor/lack of controls, and lack of product knowledge. Golden et al (2006), states that the possible causes of fraud and corruption are financial pressure, opportunity, and rationalisation and attitude. Moreover the study established that the respondents were aware of the types of frauds under the general umbrellas of Asset misappropriation, fraudulent financial statements and records, and corrupt or prohibited practices.

The study found out that preventative, training, detection, prosecution and investigation strategies would effectively mitigate the opportunity to commit fraud since an effective fraud prevention program could increase pressures and incentives to act honestly by emphasizing a “perception of detection,” underscored by the company’s demonstrated, consistent commitment to taking appropriate and certain action once fraud is discovered. KPMG (2006) advocates that an effective, business driven fraud and misconduct risk management approach is one that focuses on three objectives, namely prevention, detection and response. In relation to effective strategies in fighting fraud, the study found out that proactive fraud risk strategies were better in ensuring that the risk of detection is heightened making it easier and cheaper to manage fraud. Training was found to result in prevention as the staff and customers understand various types of frauds in addition to sensitization of personnel on fraud trends. Effective prosecution on the other
hand was found to be an effective deterrent to fraud. ACFE (2003) contends that constant vigilance against fraudulent and corrupt activities mitigates the impact of fraud and corruption on organisational revenue.

The level of staff involvement in the fraud process was found to be high. Failures in control such as poor internal controls, control-related issues such as inadequate staffing, financial difficulties of employees, staff financial over commitment and inadequate reward strategies were found to increase the opportunity for employee fraud. PricewaterhouseCoopers (PwC) (2009), states that organisations must be aware of their culture as this has a bearing on the behaviour of the employees towards fraud and corruption.

Technological systems upgrades are done as and when it is necessary. This indicates that the respondent banks are continuously aware of the changes in their external environment brought about by the fast changing technology, that they scan the environment and are quick and nimble to respond to these changes. The same awareness in the changes in the operating environment was noted with regard to the frequency of updating the banks’ internal controls and operating procedures. Training was found to be a major contributor to preventative response strategies. Lister (2007) argues that in setting the tone, new employees are offered training by anti-fraud and corruption specialists during the induction process.

All the respondent banks went through some growth in the last 5 years through expansion in existing markets, new distribution channels or identification of new market segments. During this period it was established that fraud was effectively and adequately addressed.
According to Deloitte Touche Tohmatsu (2003) fraud and corruption within the organisation can translate into negative perceptions and impose reputational risk on an entity.

Top management were found to be extremely concerned with fraud prevention and detection. PwC (2009) support the view that organisations have to set the right “tone at the top”. Further, fraud investigations in the respondent banks were found to be successful and the banks have an effective investigation and prosecution policy. A reputation of aggressively investigating indications of fraud can have a strong deterrent effect. The study also found out that there exists an enforceable Fraud Policy in all the respondent banks. ACFE (2003), points out that a strong written policy should have definitions of the actions that constitute fraud and corruption, the responsibilities of the board, management, staff, internal audit and investigating staff regarding the management of fraud and corruption risks.

The study found out that the respondent banks consistently demonstrate their commitment to a zero-tolerance policy with support for prosecution (impartial treatment) of any person found to have been engaged in fraudulent activity. Petrosa (2010) states that policies must be clear and written in simple language and should include a statement that the organisation is committed to zero tolerance aimed at eliminating fraud and corrupt activities. The study further established that the banks were properly equipped in terms of employee know how on fighting fraud with clearly determined reporting responsibilities and management authority and awareness amongst all members of staff that they were responsible for preventing fraud. Golden et al (2006), says that fraud and corruption can be deterred by establishing good corporate governance.
CHAPTER FIVE: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presents the summary of the data findings on the response strategies to fraud by the listed commercial banks in Kenya, the conclusions and recommendations are drawn there to. The chapter is therefore structured into summary of findings, conclusions, recommendations, limitations of the study and suggestions for further research.

5.2 Summary of Findings

The following paragraphs present a summary of the findings.

While all the respondents worked for various listed banks, there was a high level of non-disclosure of the bank for which they worked. This can be attributed to the sensitivity of the issue being researched on. More males were found to have been tasked with the responsibility of implementing fraud response strategies than their female counterparts. In addition the respondents were found to have the appropriate experience and knowledge of managing fraud. The findings also pointed out majority of the respondents were in senior management level and middle management levels, hence could be relied upon to give accurate information on response strategies to fraud by the listed commercial banks in Kenya.

The respondents are very familiar with the scope of the risks to be managed encompassing credit cards, fixed deposits, mortgage products, savings accounts, current accounts and mobile banking. The study also instituted that the respondents were up to date with the necessary skills required as they were recently trained on them. This kind of
participation helps members to identify and anticipate changes that are happening in the environment. Additionally, the study ascertained that the respondents’ banks have a whistle blowing facility for purposes of raising a red flag; a key response strategy. The study further revealed that the banks undertake frequent employee training on fraud thereby keeping the subject alive and also equipping the staff with the necessary skills to respond to fraud. The study also found that the pressures that often motivate fraud are staff frustrations, poor/lack of controls, and lack of product knowledge.

The listed banks have adopted the following response strategies to fraud; prevention, training, detection, prosecution and investigation strategies to effectively frustrate/mitigate and manage fraud in their banks. In relation to effective strategies in fighting fraud, the study found out that proactive fraud risk was better in ensuring that the risk of detection is heightened and in the final end it becomes easier and cheaper to manage fraud with regard by adopting preventive strategy. Training as a prevention strategy was said to focus on equipping staff with the right skills and knowledge to identify fraudulent attempts. Whistle blowing as a preventive strategy raises the flag before the fraud is attempted. Moreover, prosecution was found to be a deterrent strategy that sends the message that fraudsters will be prosecuted.

The level of staff involvement in the fraud process was found to be high. Failures in control such as poor internal controls, inadequate staffing, financial difficulties of employees such as financial over commitment and inadequate reward strategies were found to increase the opportunity for employee fraud.
Technological systems upgrade needs to be done as and when it is necessary because with the changes in the external environment brought about by fast changing technology, the listed banks must scan the environment and be quick and nimble to respond to these changes. The same case was identified with regard to frequency of review of the bank’s internal controls and procedures updating. Regarding pre-employment screening, the bank’s pre-employment screening was found to be very rigorous commensurate with the company’s fraud risk and take into account applicable legal considerations.

The banks growth in the last 5 years was found to involve expansion in existing markets, new distribution channels and identification of new market segments. During this period it was established that fraud was effectively and adequately addressed. The law enforcement agencies were found to be moderately effective in the fight against fraud. On the other hand, the fraud investigations in the respondent banks as measured by successful apprehension of fraudsters were found to be successful. The banks were found to have an effective investigation mechanism in place.

The respondent banks demonstrate their commitment to a zero-tolerance policy with support for prosecution (impartial treatment) of any person found to have been engaged in fraudulent activity. Besides this, the study established that the top management was extremely concerned about fraud prevention / detection. The study further established that the banks were properly equipped in terms of employee know how on fighting fraud with clearly determined reporting responsibilities and management authority and awareness amongst all members of staff that they were responsible for preventing fraud. The study also found out that there exists an enforceable of bank Fraud Policy among the organisations.
Finally the study established that recommendations such as investing in supporting technology, screening of new employees, training officers on IT investigations as the current fraud trends are through internet banking-electronic frauds, enforcing internal controls, emphasizing on KYC and customer due diligence before opening bank accounts, embracing new technology of EMV-chip cards, judiciary reform to ensure prosecution of offenders and sharing of lessons learnt would help banks to reduce level of fraud.

5.3 Conclusion

The following are the conclusions from the study.

The listed commercial banks have in place various response strategies to manage the different types of fraud that face them. These range from preventative strategies to detective, investigative to deterrent strategies. It is also evident that all staff in these banks are empowered to be at the fore front of fighting/managing fraud in their various roles.

Top management take fraud seriously and therefore it is concluded that the tone at the top in all the respondent banks is that of zero-tolerance to fraud. All the respondents are well experienced, understand the different types of fraud and have fraud as a performance metric in their performance contracts. The existence of a fraud policy ensures that staff are aware of their role, responsibilities, expected action and escalation of fraud related challenges. The listed banks have further created an avenue for staff to raise the flag via the whistle blowing policy. This creates the necessary confidence levels that genuine concerns on fraud can be brought to the attention of the heads of fraud without the whistle blower exposing themselves or putting themselves at risk. Fraud training is done
frequently to keep staff abreast of new and emerging frauds and modes of operations of the fraudsters. While the law enforcement agencies play a critical role in terms of investigating, apprehending, prosecuting and sentencing of the fraudsters, it was found that their level of effectiveness was average.

All the banks had undergone some form of growth or expansion in the last five years. The changes ranged from expansion in terms of branch network, entering new markets and introduction of new products and services. This meant recruitment of new staff, getting new customers, introducing new technologies etc. Yet it was concluded from the study that during this period of change fraud was managed effectively. The strategy of taking customers through strict know your customer and customer due diligence processes, pre-screening of new staff and regular auditing are other strategies that the respondent banks have adopted.

Listed banks like all other organisations operate within an environment. They continuously scan this environment and adequately respond to changes in their operating environment. This is demonstrated by the fact that technological changes/upgrades are done as and when necessary. Policies and procedures are also reviewed as and when necessary. This means that the banks operating procedures remain update and fit for purposes throughout.
5.4 Recommendations for Policy and Practice

Due to the diverse nature of businesses and organizations, implementing a fully standardized approach to fraud would not be feasible or practicable. There are, however, a number of key best-practice policies and procedures that the study recommends that the listed commercial banks should consider.

The study brought out the need for a database to be established of persons who have committed fraud in the past and this should be shared amongst banks to ensure that such individuals are not offered the opportunity to open accounts that are meant to facilitate fraud. All the banks should fast track the adoption of chip technology in their credit card and debit card products. This technology has reduced fraud in other countries and hence the need to adopt it going forward.

As fraud continues to evolve and become more technology driven, it is our recommendation that the investigating officers both in the listed commercial banks and the law enforcement agencies are continuously up skilled in this area particularly in technologically driven fraud. This could be done jointly for purposes of creating synergy in the area of fraud management.

Undertaking background checks before employing staff is a critical strategy to manage fraud. It is our recommendation that this be made mandatory as our study revealed that certain respondent banks did not undertake rigorous pre-screening of new staff. While know your customer requirements have been adopted by all the respondent banks, a key challenge continues to be the authenticity of the documents presented for account
opening. Instances of accounts opened using fake documentation are reported routinely in the local press.

Our recommendation is for a review of the security features of the identification documents to be undertaken and if possible include biometrics at the point of issuance. There is a need to fast track the reforms in the police sector and the judiciary. This will help in faster turnaround times in the investigations, prosecution and sentencing of the fraudsters. This would act as a deterrent to potential fraudsters

5.5 Limitations of the Study

From the questionnaires response, 60% of the respondents did not disclose the organisations they work for. This is because of the sensitive nature of the topic under study.

It’s also important to note that the data collected from the respondents may have suffered from personal biases of the respondents and may therefore not have fully represented the response strategies in the listed banks in some cases.

5.6 Suggestions for further Research

In order to deal with the issue of personal bias, further research using a different form of data collection e.g. face to face interviews should be undertaken. This would present the researcher with the opportunity to ask probing questions or seek clarifications and explanations to certain specific questions that may otherwise be inadequately responded to when a questionnaire is used.
Fraud is a major cause of concern not just in the banking industry but also in other sectors as well e.g. mobile phone companies which have become major providers of money transmission services, insurance companies etc. Research should be undertaken to determine the existence or otherwise of any common themes in terms of mode of operation, response strategies etc. Another area would be to determine whether there are demographic considerations among fraudsters in terms of age, gender or educational background and the type of fraud committed. This could help banks come up with specific response strategies to specific types of fraud.
REFERENCES


Banking Fraud and Investigations Department, (2012), *Quarterly Banking Fraud statistics*, 4.


## APPENDICES

**Appendix I: List of Listed Commercial Banks in Kenya as at 30th September 2013**

<table>
<thead>
<tr>
<th></th>
<th>Bank Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Barclays Bank of Kenya Ltd (BBK)</td>
</tr>
<tr>
<td>2</td>
<td>CFC Stanbic Bank</td>
</tr>
<tr>
<td>3</td>
<td>Equity Bank Ltd</td>
</tr>
<tr>
<td>4</td>
<td>Housing Finance</td>
</tr>
<tr>
<td>5</td>
<td>Kenya Commercial Bank Ltd</td>
</tr>
<tr>
<td>6</td>
<td>National Bank of Kenya Ltd</td>
</tr>
<tr>
<td>7</td>
<td>NIC Bank Ltd</td>
</tr>
<tr>
<td>8</td>
<td>Diamond Trust Bank (DTB)</td>
</tr>
<tr>
<td>9</td>
<td>Cooperative Bank of Kenya Ltd</td>
</tr>
<tr>
<td>10</td>
<td>Standard Chartered Bank Ltd</td>
</tr>
<tr>
<td>11</td>
<td>I&amp;M Bank</td>
</tr>
</tbody>
</table>

*Source (Nairobi Securities Exchange, 2013)*
Appendix II: Questionnaire

This questionnaire seeks to collect data on response strategies to fraud in Listed Banks in Kenya. All information received will be treated confidentially and will be used for academic purposes only.

Section A: Background

1. Personal Information

   Please indicate
   
   a) Name of Bank: .................................................................

   b) Gender:     Male .................... Female ..............................

   c) Working experience
   
   Less than 1 year (  ) 1-5 yrs (  ) 6-15 years (  ) Over 15 years (  )

   d) Level: Clerical (  ) Supervisory (  ) Middle Management (  ) Senior Management (  )

Section B:

2. Which of the following products are you familiar with?

   Credit Cards (  ) Fixed Deposits (  ) Mortgage Products (  )

   Savings Accounts (  ) Current Accounts (  ) Mobile Banking (  )

3. When were you last trained on these products?

   Less than 1 year (  ) 1-5 yrs (  ) 6-15 years (  ) Over 15 years (  )

4. Does your Bank have a Whistle Blowing Policy?

   Yes (  ) No (  ) Don’t Know (  )

5. How frequently is Fraud training conducted?

   Quarterly (  ) Half-Yearly (  ) Annually (  ) Never (  )

6. What in your view are the leading causes of fraud in the bank? (Tick as appropriate)

   • Staff frustrations (  )

   • Lack of controls within the different processes (  )

   • Insufficient procedures (  )
7. What are the types of fraud that you know?

- Theft and Embezzlement ( )
- Defalcation ( )
- Forgeries ( )
- False Identity ( )
- Unofficial Borrowings ( )
- Money Laundering ( )
- Card Fraud ( )
- Fake payments ( )
- Computer fraud ( )

8. What in your view is the most effective strategy in fighting fraud?

   Prevention ( ) Detection ( ) Investigation ( ) Prosecution ( ) Training ( )

   Please elaborate…………………………………………………………………………

9. In your view what is the level of staff involvement in the fraud process?

   Very High ( ) High ( ) Moderate ( ) Low ( ) None ( )

10. What in your opinion are the major factors contributing to fraud in listed Banks?

   Inadequate staffing ( )
   Poor internal controls ( )
   Lack of staff training ( )
   Inadequate reward strategies ( )
   Financial Over commitment ( )
   High staff turnover ( )

11. How often are your technological systems upgraded?

   Every 2 years ( ) Annually ( ) Every 6 Months ( ) As & when it is necessary ( )
   Not sure ( )
12. How often are internal controls and procedures updated in the bank?
   Every 2 years ( ) Annually ( ) Half-yearly ( ) As & when it is necessary ( )
   Not sure ( )

13. How rigorous do you consider pre-employment screening in your bank to be?
   Very Rigorous ( ) Above Average ( ) Below Average ( ) Does not exist ( )

14. How has the Bank grown in the last 5 years?
   Expansion in existing markets ( )
   Identification of new market segments ( )
   Through mergers and acquisitions ( )
   New Products ( )

15. Was fraud in your view effectively addressed during this growth period?
   Effectively addressed ( ) Adequately addressed ( ) Moderately addressed ( )
   Not Addressed ( )

16. How would you rate the success of the law enforcement agencies in the fight against fraud?
   Very Successful ( ) Successful ( ) Averagely Successful ( ) Below Average success ( )
   If your answer is below average success, please give a brief commentary to support your view
   ……………………………………………………………………………………………
   ……………………………………………………………………………………………
   ……………………………………………………………………………………………

17. How effective do you consider Fraud investigations in your bank to be?
   Very Effective ( ) Effective ( ) Average ( ) Below Average ( ) Non-existent ( )

18. Do you consider the level and depth of investigations to be adequate?
   Yes ( ) No ( ) Don’t Know ( )
19. In your view is the top management concerned about fraud prevention / detection?
   Extremely ( )  moderately ( ) Below Average ( ) Not concerned ( )

20. To what extent does your bank employ the following strategies to combat fraud?
   **Key**
   
   5 = To a Very Great Extent 4 = To a Great Extent
   
   3 = Moderate Extent 2 = Little Extent
   
   1 = Not at all

<table>
<thead>
<tr>
<th>Statement</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application of Know Your Customer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Screening of new staff</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Periodic fraud training to employees</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regular auditing of transactions by internal and external auditors</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adoption of new technology</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Whistle Blowing facility</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application of strong internal controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other (please specify)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

21. How do you rate your level of knowledge in fighting fraud in your current role?
   Very High ( )  High ( )  Moderate ( )  Low ( )  Poor ( )

22. Does Fraud management form part of your Performance Contract/ do you have responsibility to fight/manage fraud?
   Yes ( )  No ( )  Not Sure ( )
23. In your view who is responsible for preventing fraud in the Bank?
   Clerical staff ( ) Middle level Management ( ) Senior Management ( ) All staff ( )

24. Does the Bank have a Fraud Policy and in your view is it enforced?
   Yes ( ) No ( ) Don’t Know ( )

What recommendations would you give the bank to help reduce level of fraud?

........................................................................................................................................
........................................................................................................................................
........................................................................................................................................

Thank you for taking time to answer this questionnaire